SANDIA REPORT
SAND2000-3007
Unlimited Release
Printed December 2000

Directory-Enabled Networking Design Reference

Curtis M. Keliiaa

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2000-3007
Unlimited Release
Printed December 2000

DIRECTORY-ENABLED NETWORKING DESIGN REFERENCE

Curtis M. Keliiaa
Telecommunication Operations Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0812

Abstract

The purpose for presenting a directory-enabled design philosophy is to emphasize the role of directory service technologies as the foundation for scalable, secure information exchange. Directory services are at the core of intelligent networks. This document is intended as a design reference for enterprise directory implementation and was written to address the fact that directory-service technologies are impacting every aspect of network computing. Major industry vendors have based current and future product direction on directory-service technologies. Directory-service product vendors include Novell, Microsoft, Sun/Netscape Alliance, Oracle and Cisco Systems.

Industry standards provide the fundamental guidelines for directory interoperation scalable to global networks. At issue is the heterogeneous nature of large enterprise and global networks. A large enterprise or global network environment imposes the consideration of supporting multiple computing platforms, sites and business-operation models. This report is written to improve understanding and clarify the issues and complexities of designing and implementing directory services in a heterogeneous large-scale network-computing environment.

Acknowledgements

The information presented in this report is based on the experience of the author as a commercial consultant, a network administrator, and as a Telecommunication Operations network designer in the Sandia network-computing environment. This experience includes:

- Novell CNE, Microsoft MCSE and Cisco CCNA certifications
- Sandia Material And Process Sciences Network (MAPSNet) Novell NetWare 3.12 & 4.11/Novell Directory Services network management
- The 1996 Sandia Novell Directory Services, Microsoft NT, UNIX and Apple Macintosh over the TCP/IP transport unified design
- Sandia Corporate Server Microsoft Windows NT 3.5 & 4.0 server management
- Sandia Telecommunication Operations Corporate Cisco Intranetwork design
- Windows 2000 coursework and research
- Industry standards and protocol research

This work is a compilation of effort, which over time involved collaboration with many individuals and groups. I would like to express my appreciation to the professionals that I have had the great fortune to work with and learn from. This includes those on the Sandia Corporate Server Team, CSU Technical Development Team, Computer Security, Server Consistency Team, Telecommunication Operations Network Design Team and the Advanced Network Integration group.

I would like to express my gratitude to David Evans, Ed Klaus and Tim MacAlpine, the old MAPSNet crew, for their continued insightful, trusted and valued contributions.

I would like to express my gratitude to Anne Van Arsdall of the Sandia Telecommunication Operations Department for her thoughtful and professional commentary and editing.

I would like to express my gratitude to Steve Gossage of the Sandia Advanced Network Integration group for his guidance and encouragement.

My appreciation goes to the technical reviewers for taking the time and consideration to help ensure the integrity of this document.

Detailed information on specific vendor products is beyond the scope of this document. Please refer to the Technical References portion of this document for additional information concerning industry standards, specifications and vendor product information. This document does not endorse a specific vendor product preference. The objective of this document is to impart some measure of practical design methodology and provide an understanding of the risks, complexities and most importantly the benefits of directory-enabled networking. The information and recommendations presented in this document are based on the technical opinions and research of the author and do not imply technical reviewer concurrence with the content.

Curtis M. Keliiaa

Contents

List of Figures

Appendices

EXECUTIVE SUMMARY

Directory-service technologies provide a scalable, logical canopy for all elements of a network, including its physical, logical and policy elements. Industry vendors having invested in directory-service technologies include Microsoft, Sun/Netscape Alliance, Oracle, Novell, Lucent Technologies and Cisco Systems. They and industry standards bodies are pursuing directory-enabled initiatives as the foundation for universal connectivity. In addition, the Internet Engineering Task Force (IETF) and the Distributed Management Task Force (DMTF) are collaboratively developing industry standards to integrate network management and policy-based networking.

Integrated, intelligent management of all network elements requires that profiles and policies manage users, applications, workstations, network devices, and network services. A profile represents a set of attributes that describes the requirements and characteristics of a client (user or application) of a network service. A policy represents the aggregate associations of logically represented network elements and element attributes that describe client access (who, how, when and where) to network resources and services.

Two structures are necessary to represent network elements logically: an information model and a directory name space. An information model provides a consistent manner to model network elements, and a directory-service name space provides the hierarchical structure for logical objects. The information model that maps to the directory name space provides integration permitting intelligent management of network resources. Policy-based networking leverages this information model to facilitate secure, intelligent network management.

Directory-service technologies enable secure, integrated information exchange, network management, and user administration. They provide the technologies for comprehensive network management, superior security posture, and integrated user administration, which facilitates reduction in the total cost of ownership. The most significant advantage of implementing a well-planned directory-service architecture is the functional surety gained by the association or relationships of logically represented objects. This surety in turn enables:

- Superior network resource accessibility
- Integrated management of web-based resources
- Network service provision
- Integrated management of servers and applications
- Superior security model
- Policy-based-networking
- Automated desktop and application configuration based on machine ID or login ID
- Automated network device configuration based on conditional parameters

The resulting integrated management methodology produces more efficient use of network resources. A philosophy of directory-enabled networking design embraces directory service technologies that have become the industry basis for intelligent, secure integrated network management.

INTRODUCTION

This document presents a standards-based ideology for an enterprise or multi-organizational directory-service architecture. The heterogeneous nature of a multiple organization collaborative network-computing environment mandates that an industry standards-based approach is adopted in the design of a directory-service architecture. An integrated directory-service design would facilitate secure collaborative science and engineering and provide the foundation for manageable geographically distributed networks.

Objectivity in presenting this information is based on the following considerations:

- Vendor independence
- Standards-based design philosophy
- Directory interoperability
- Whole environment approach—organizational, operational and user stratification with respect to network security and network resource accessibility
- Peer review

The intent of this report is to provide a general understanding of the issues and complexities in a standards-based directory-enabled networking design philosophy.

Directory-Enabled Networking Design Philosophy

The proliferation of the Internet, distributed web-based applications, electronic commerce and the increasing dependence of today's workplace on technology have accelerated the need for a comprehensive network-computing management strategy. It is necessary not only to manage and protect information, but also to enable information exchange and secure data access.

When considering information exchange with collaborative partners who function under different authority or business models, several questions arise. How do you control who has access to sensitive information when the user is beyond the security barriers of your network? How do you allow collaborative computing and secure information exchange with trusted partners? How do you manage the type of service and quality of service for applications such as video conferencing to remote locations or with other organizations? Is there a way to manage to all of these issues securely?

Security is a fundamental concern when opening the gate to company information. Technologies such as Virtual Private Networks (VPN) and the encrypted secure HyperText Transfer Protocol (HTTPS) provide point-to-point secure communication over the Internet. But what about the larger issues of connecting multiple organizations that need to collaboratively communicate?

Directory-service technologies provide the means to manage information, user identity, applications, and network services for the complete network. This is accomplished through logical representation of network elements. The logical representation of all types of network elements allows for secure, scalable management. Country, geographic location and organization are also represented as logical objects in a directory.

The introduction of directory service technologies into large network computing environments requires careful evaluation, planning and implementation. The development of an enterprise directory design requires that the needs of the network as a whole be considered. Business processes, user stratification, computing platforms, e-commerce, distributed applications, network services and security must be factored into the directory design. Leveraging a directory service for policy-based networking requires that application distribution, network traffic characteristics and service client requirements are identified, quantified and prioritized. Industry standards-based design and common design strategies facilitate directory interoperation. A directory enabled design philosophy incorporates these ideals into the network design process.

Directory Services In A Nutshell

A directory service consists of a schema that defines object classes and attributes. The directory schema consists of an information model that defines network elements as logical objects. The information model provides a consistent manner in which to represent network elements. The directory represents a name-space for logically represented network elements. The name-space logical structure is hierarchical and scalable. For example countries, organizations, departments, users, workstations, servers, applications, network equipment, protocols, policies and network services are represented as logical objects as illustrated in Figure 1.

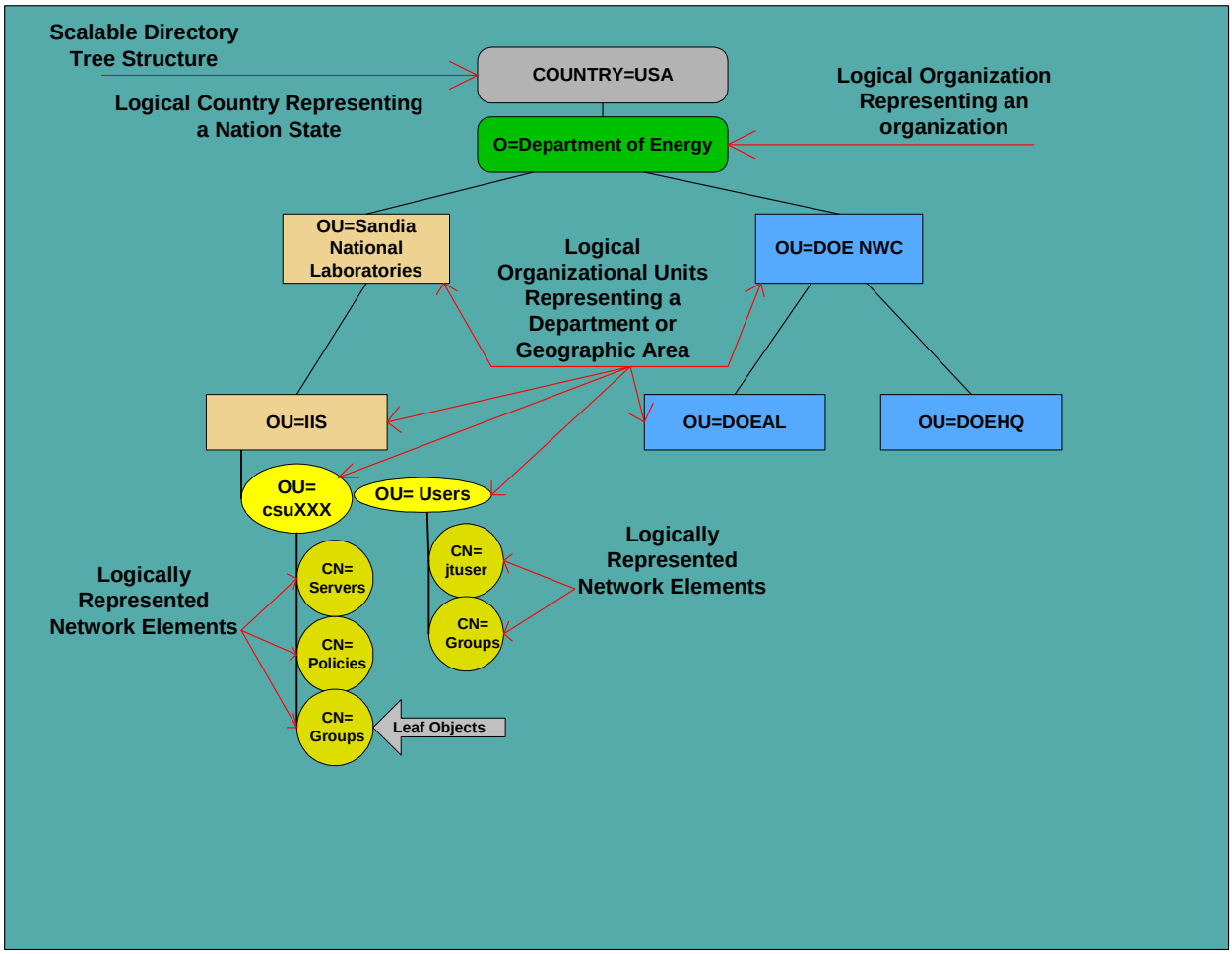

Figure 1

Directory-service technologies enable secure integrated information exchange, network management and user administration. A directory service allows for a superior security posture through logical security boundaries that overlay physical, file-system and network-operating system security. For example the directory has rights and permissions that add another layer of control in addition to network-operating system and file-system security. Logical objects are secured with access control lists, access control entries and directory permissions. This logical hierarchy is further partitioned into autonomous areas of administration by means of directory-object permissions, attributes and associations. A scalable, secure directory structure with logical security boundaries is illustrated in Figure 2.

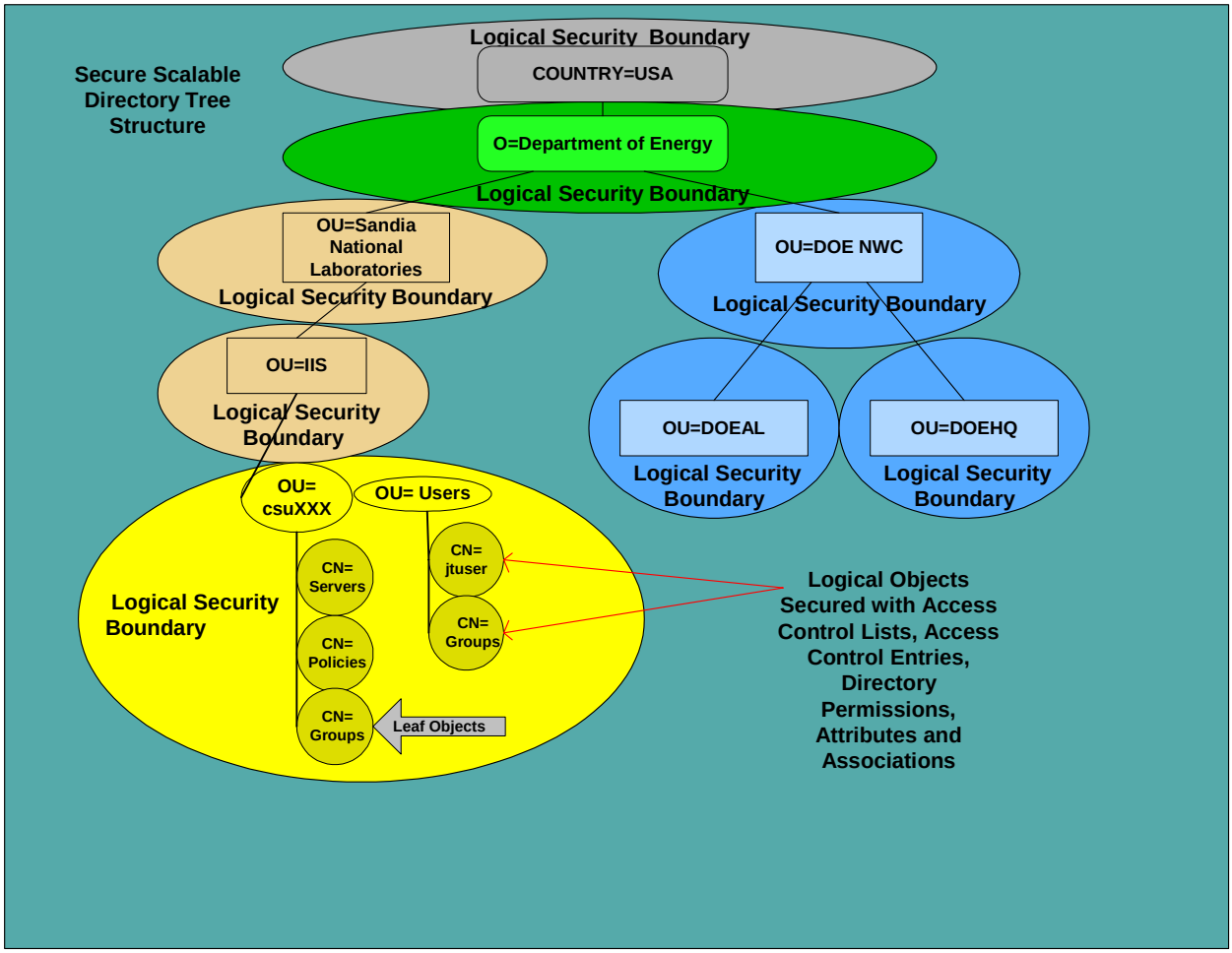

Figure 2

Logical-object associations in conjunction with conditional parameters of network elements provide the structure for policy-based networking. Policies can be global, regional or local and apply to user accounts, machines or services for access control. Policy-based networking allows integrated service provision and configuration of network elements. Directory services ensure a greater security posture and network-management efficiency by means of a thorough network-element information model.

In the pages that follow, directory-service technologies are studied and presented with a focus toward a DOE NWC collaborative network-computing environment.

Technical Reviewers

Bruce Whittet - Sandia Network Design Group Telecommunication Operations
Ed Klaus - Sandia Network Design Group Telecommunication Operations
Roger Adams - Sandia Network Design Group Telecommunication Operations
Vicki Williams - Sandia Network Design Group Telecommunication Operations
Pat Torrez - Sandia Network Design Group Telecommunication Operations
Steve Gossage - Sandia Advanced Network Integration
Larry Tolendino - Sandia Advanced Network Integration
Tim MacAlpine - Sandia Corporate Server Management Team, Microsoft Systems
Mark Stilwell - Sandia Corporate Server Management Team, Microsoft Systems
David Evans - Sandia Applications Analysis Telecommunication Operations
Jay Smith - Sandia Applications Development
Doug Brown - Sandia Computer Security
Darrel Patrick - Sandia Computer Security
Roger Suppona - Sandia Computer Security
Carlos Quintana - Sandia CSU Technical Development
Mark Gutscher - Sandia Corporate Server Team, UNIX Systems
Jim Muntz - Sandia Corporate Server Team, UNIX Systems
Jerry Esch - Sandia Database Administration and Program Management
Rich Gay - Sandia Network Design Group, Livermore California

Editorial Reviewers

Michael Sjulin - Sandia Telecommunication Operations Manager
Anne Van Arsdall - Sandia Telecommunication Operations Technical Writer

Directory Enabled Networking Executive Summary Reference URL

The Directory Enabled Networking Executive Summary can be reviewed on the Sandia Restricted Network Web FileShare at the following URL:
HTTPS://wfsprod01.sandia.gov/groups/srn-uscitizens/documents/document/wfs017669.pdf

Directory Enabled Networking Technical Summary Reference URL

The Directory Enabled Networking Technical Summary can be reviewed on the Sandia Restricted Network Web FileShare at the following URL:
HTTPS://wfsprod01.sandia.gov/groups/srn-uscitizens/documents/document/wfs021637.pdf

This document - The Directory-Enabled Networking Design Reference can be reviewed on the Sandia Restricted Network Web FileShare at the following URL:
HTTPS://wfsprod01.sandia.gov/groups/srn-uscitizens/documents/document/wfs014117.pdf

DIRECTORY SERVICE TECHNOLOGIES

Directory services provide a means to represent all network elements logically in a scalable hierarchical name-space. The industry development of directory-service technologies is impacting every aspect of managing an enterprise-computing environment. Directory services are a fundamental component of every major current network-operating system and therefore are key in providing network and computing services. Directory-service technologies enable identity and profile management, which are critical to business-to-business and business-to-customer e-commerce. The Internet Engineering Task Force X.500 Distributed Directory specification is the standards-based foundation for today's directory-service solutions. The X.500 protocol suite supports X.400 and other messaging systems but is not limited to e-mail services.

There are many directory-service product offerings available on the market today. The DOE and affiliated national laboratories could leverage these technologies to build an e-science infrastructure to support the DOE NWC network-computing environment. In addition to Microsoft Active Directory, Novell Directory Services eDirectory and Sun/Netscape Alliance iPlanet Directory Server, other industry Lightweight Directory Access Protocol server products include:

- Computer Associates eTrust Directory
- Critical Path Global Directory Server
- Innosoft/Sun IDDS
- Open Source OpenLDAP
- Oracle Internet Directory
- Siemens DirX

In addition, integrated solutions and directory bridging technologies are available. Oblix, Inc (http://www.oblix.com) offers Oblix Service Center and Oblix Publisher, which integrate LDAP-server information and manage user profiles. Access360 (http://www.access360.com) enRole bridging software product provides access to numerous system and application directories.

The Internet Engineering Task Force X.500 Distributed Directory specification (1988,1993) sets the standard and is the baseline for Novell Directory Services eDirectory and Lightweight Directory Access Protocol directory architectures. The X.500 protocol suite defines a global hierarchical structure based on country, state, city, address, and people. The major components of the X.500 distributed directory specification include:

- Directory Information Base (DIB) or white pages directory
- Directory Server Agent (DSA)
- Directory User Agent (DUA)
- DSA sites
- The 1993 edition includes replication and access control - Directory Information Shadowing Protocol (DISP)

ISO/ITU X.500 Distributed Directory Standards

The X.500 Distributed Directory specification discussion is an outline, detailed discussion is not pursued. The general architecture and functionality are presented to give a structural understanding that applies to the conceptual design of directory-services solutions.

The X.500 Distributed Directory Standards

- X.500 The Directory: Concepts Models and Services
- X.501 Models
- X.509 Authentication Framework
- X.511 Abstract Service Definition
- X.518 Procedures for Distributed Operations
- X.519 Protocol Specifications
- X.520 Selected Attribute types
- X.521 Selected Object Classes
- X.525 Replication
- X.530 Use of Systems Management for Administration of the Directory

X.500 Specification Logical-Objects

The X.500 specification defines three object types:

- Abstract Objects - One abstract object is defined. "top" and represents a set of common properties used by every object in the directory tree.

- Auxiliary Objects - Used internally by the directory tree to create structural objects.

- Structural Objects - Effective objects or object classes that form the directory tree.

Logical objects abide by the following structure:

- Class
- Type
- Attributes
- Association
- Context
- Container

The Internet Engineering Task Force X.500 Specification Leaf Objects

Leaf Objects defined by X.521:

- Application Entity
- Application Process
- Certificate Authority
- Certificate Authority -V2
- CRL Distribution Point
- Device
- Directory Management Domain
- Directory System Agent
- Group of Names
- Group of Unique names
- Organizational Person
- Organizational Role
- Person
- Residential Person
- Strong Authentication User
- User Security Information

Common computing leaf objects:

- Administrator
- Server
- Volume
- Machine
- Policy

Common Directory-Enabled-Networks/Common-Information-Model leaf-objects:

- Cabinet
- Chassis
- Circuit
- Protocol
- Service
- Policy
- Profile

The Internet Engineering Task Force X.500 Protocols

The X.500 specification protocols include:

- Directory Access Protocol (DAP)
- Directory System Protocol (DSP)
- Directory Operational Binding Management Protocol (DOP)
- Directory Information Shadowing Protocol (DISP)

In addition to the standard OSI-defined protocols X.500 utilizes the following OSI-defined standards:

- Access Control Services Element (ACSE) - used in managing directory agent associations and bind\unbind operations.

- Remote Operation Service Element (ROSE) - used in request/reply interaction between X.500 protocols.

- Abstract Syntax Notation One (ASN.1) - syntax definition for storing and exchanging information.

The Internet Engineering Task Force X.500 models are defined that illustrate what the directory is from the perspective of users and administrators.

- User Information Model
- Operational and Administrative Information Model

Similarly, the Internet Engineering Task Force X.500 models are defined that illustrate what the directory is from a functional perspective.

- Directory Functional Model
- DSA Information Model
- Directory Distribution Model
- Directory Administrative Authority Model
- Security Model

The Internet Engineering Task Force X.500 Security

The X.500 security framework is based on the directory-administrative model. Security boundaries within the directory parallel administrative boundaries. The directory functions as a security provider and a client of the security services. The directory-tree structure is the framework for assigning access rights, security permissions and defining administrative jurisdiction. Security on logical objects can be controlled at a very granular level. Security descriptors are defined for an object and are persistent when the object is moved or renamed. Administrative jurisdiction is outlined below:

- Autonomous Administration Areas (AAA) - Managed by independent organizations. Corresponds to a Autonomous Administrative Point (AAP)

- Specific Administrative Areas (SAA) - Subtrees of Autonomous Administrative Areas in which entries are viewed from a specific administrative perspective. Corresponds to a Specific Administrative Point (SAP)

- Inner Administrative Areas - Delegated administration within an organization. Corresponds to a Inner Administrative Point (IAP)

- Access Control Specific Area (ACSA) - Area defined by common access control requirements

- Access Control Inner Administrative Area (ACIA) - Nested access control, an ACIA can be nested in an ACSA or within another ACIA.

- Collective Attribute Specific Area (CASA) - Area defined by common collective attributes

Logical objects maintain Access Control Lists (ACL), Access Control Policies and Access Control Entries (ACE). Access Control Areas may be divided into sets of directory entries in a Directory Access Control Domain (DACD)

The X.509 specification defines three security services:

- Simple Authentication
- Strong Authentication
- Digital Signatures

Additionally, X.509 describes symmetric cryptography and asymmetric cryptography. The authentication framework is based on these security services for protected password, mutual authentication, and public-key cryptography processes. X.509 Digital Certificates are negotiated with a certificate authority such as VeriSign (www.verisign.com).

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol is a subset of the Directory Access Protocol (DAP). The Lightweight Directory Access Protocol defines a directory access protocol specifically over the TCP/IP suite of protocols and adheres to the X.500 directory specifications. The Lightweight Directory Access Protocol has become the de facto standard as a baseline for directory-service implementation. Novell, Microsoft and Sun/Netscape Alliance directory-service products are LDAP version-3 compliant. The X.500 specifications and LDAP provide the foundation for building a unified directory-service design. A brief outline is provided to illustrate the LDAP architecture. For further information, consult the following IETF Request for Comment documents:

- RFC-1777 Lightweight Directory Access Protocol.
- RFC-1558 A String Representation of LDAP Search Filters
- RFC-1778 The String Representation of Standard Attribute Syntaxes
- RFC-1779 A String Representation of Distinguished Names
- RFC-1798 Connectionless LDAP
- RFC-1823 The LDAP Application Program Interface
- RFC-1959 An LDAP URL Format

Directory Access Operations are as follows:

- Read
- List
- AddEntry
- ModifyEntry
- RemoveEntry
- ModifyRDN (Relative Distinguished Name)
- Search
- Abandon

LDAP is a sibling protocol to HTTP and FTP and uses the ldap:// prefix in its URL.

Lightweight Directory Duplication/Replication/Update Protocols (LDUP)
The LDAP Replication Architecture and Replication Information Model provides the definition for:

- Consistency models
- Replication topologies
- Replication agreements
- Administration and management of deleted objects and their states
- LDAPv3 Replication Information Transport Protocol
- LDAPv3 mandatory replica management
- LDAPv3 update reconciliation procedures
- LDAPv3 profiles
- LDAPv3 Master-Slave directory replication
- LDAPv3 Multi-Master directory replication

Lightweight Directory Interchange Format (LDIF)
LDIF: Supports the proposed Internet standard, Lightweight Directory Interchange Format for bulk loading.

Microsoft Active Directory Service

Microsoft Active Directory is a first-generation directory-service technology. Microsoft Active Directory provides a scalable directory-service solution for Microsoft Windows 2000 clients and servers. Microsoft Active Directory administration is done through the Microsoft Management Console that supports snap-in modules for a versatile, easy-to-use single point of administration. Microsoft Windows 2000 offers superior application integration including Internet-Information Services, BackOffice Systems Management Server 2.0, Microsoft SQL Server, Microsoft Office 2000 and third-party support.

A Microsoft Active Directory tree is modeled after the DNS specific-use directory tree and therefore does not adhere to the X.500 specification. Product functionality is outlined in the Novell Directory Service eDirectory & Microsoft Active Directory Service Product Feature Comparison.

Domain Name System Domain Hierarchy

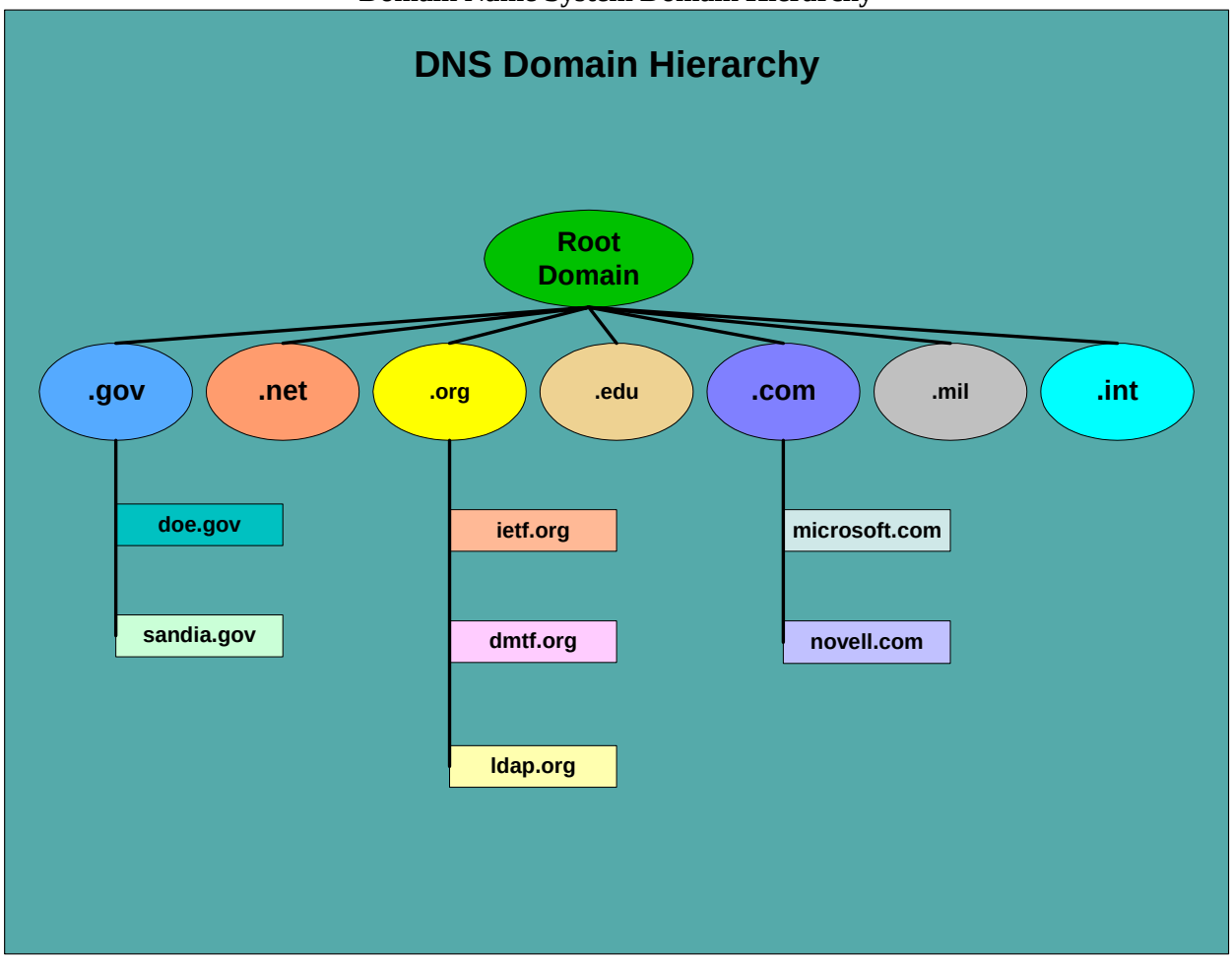

Figure 3

Microsoft Active Directory/DNS integration requires BIND 8.1.2 or later for dynamic DNS.

Microsoft Active Directory Tree Structure

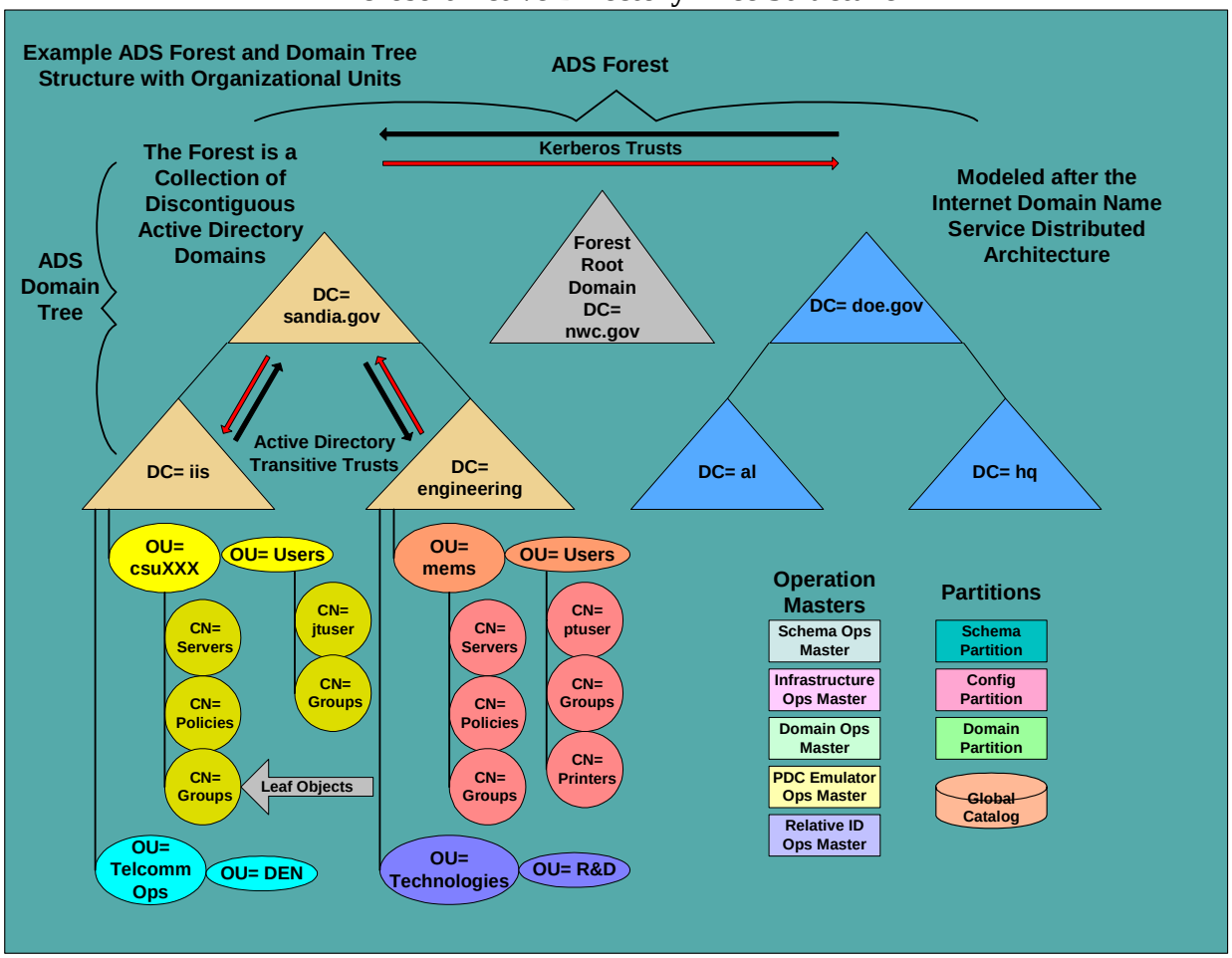

Figure 4

An Active Directory tree is a set of contiguous hierarchical domains modeled after the DNS domain structure. An Active Directory forest is a set of discontiguous Active Directory domains (a collection of Active Directory trees). Active Directory maintains transitive domain trusts throughout a directory tree that permit users and groups within the tree to access directory tree resources. Kerberos transitive trusts are maintained between the top level Active Directory tree domains within the forest. The Active Directory forest shares a common schema, configuration partition and a global catalog.

The following illustration depicts the network service environment of Sandia National Laboratories with Microsoft Active Directory represented just under the business process layer. This underscores the significance that the directory tree should closely fit the business processes and operations model of the working environment.

Sandia Active Directory Enabled Environment

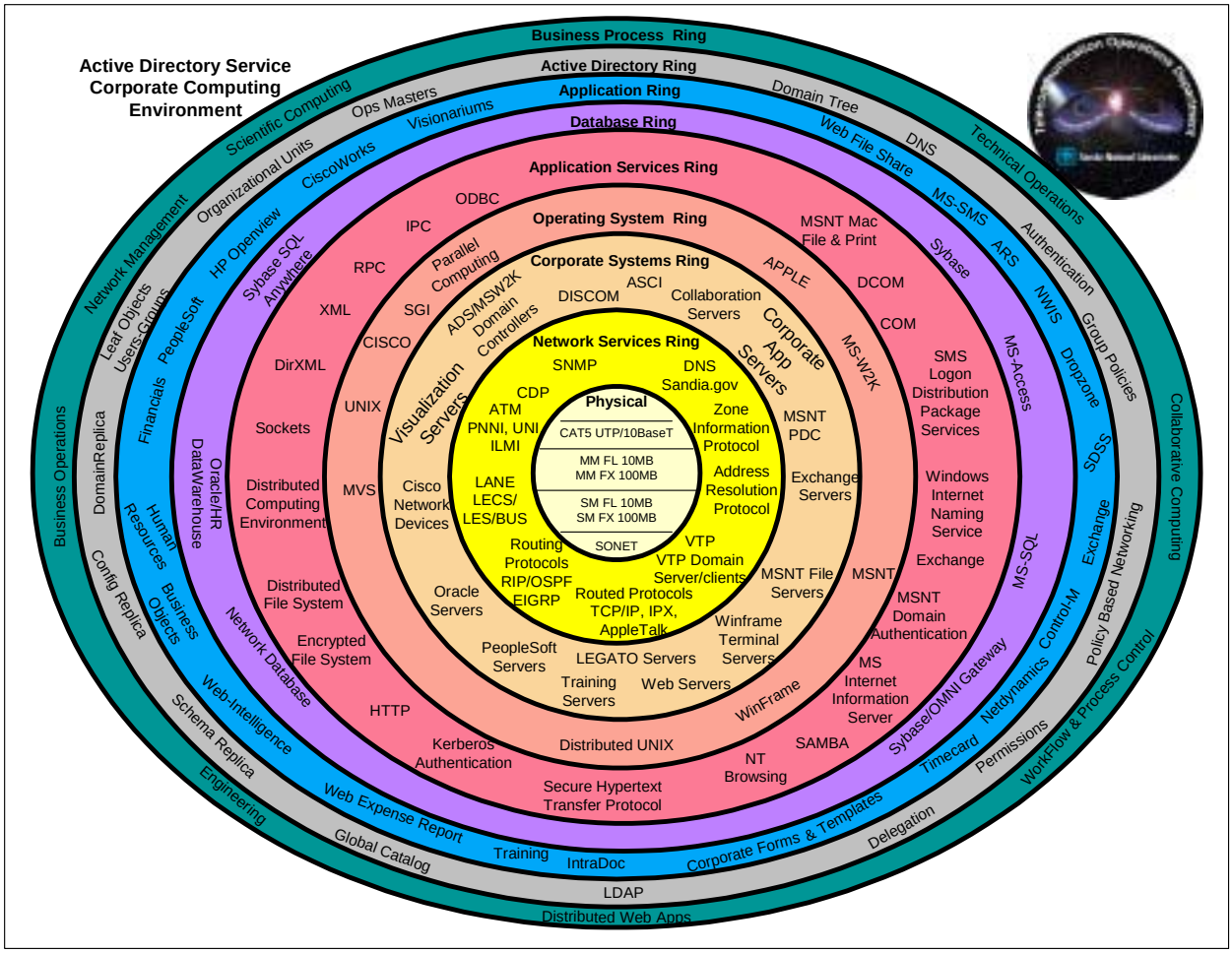

Figure 5

Novell Directory Services eDirectory

Novell Directory Services eDirectory has a strong client offering with clients for Apple Macintosh, UNIX, Linux and Microsoft variations including Windows 2000. When Microsoft NT domain architecture is a component then Novell offers NDS for NT, which replaces the Microsoft samserv.dll and redirects authentication requests to Novell Directory Services eDirectory. Novell has significant support for interoperability and actively pursues open standards including:

- Directory Interoperability Forum
- LDUP Working Group
- Directory-Enabled Networks

The interoperability with various computing platforms mixed with the maturity, scalability and open-standards support are the reason Novell Directory Services eDirectory is the leading directory service available. Product functionality is outlined in the Novell Directory Services eDirectory & Microsoft Active Service Directory Product Feature Comparison.

Novell Directory Service eDirectory Tree Structure

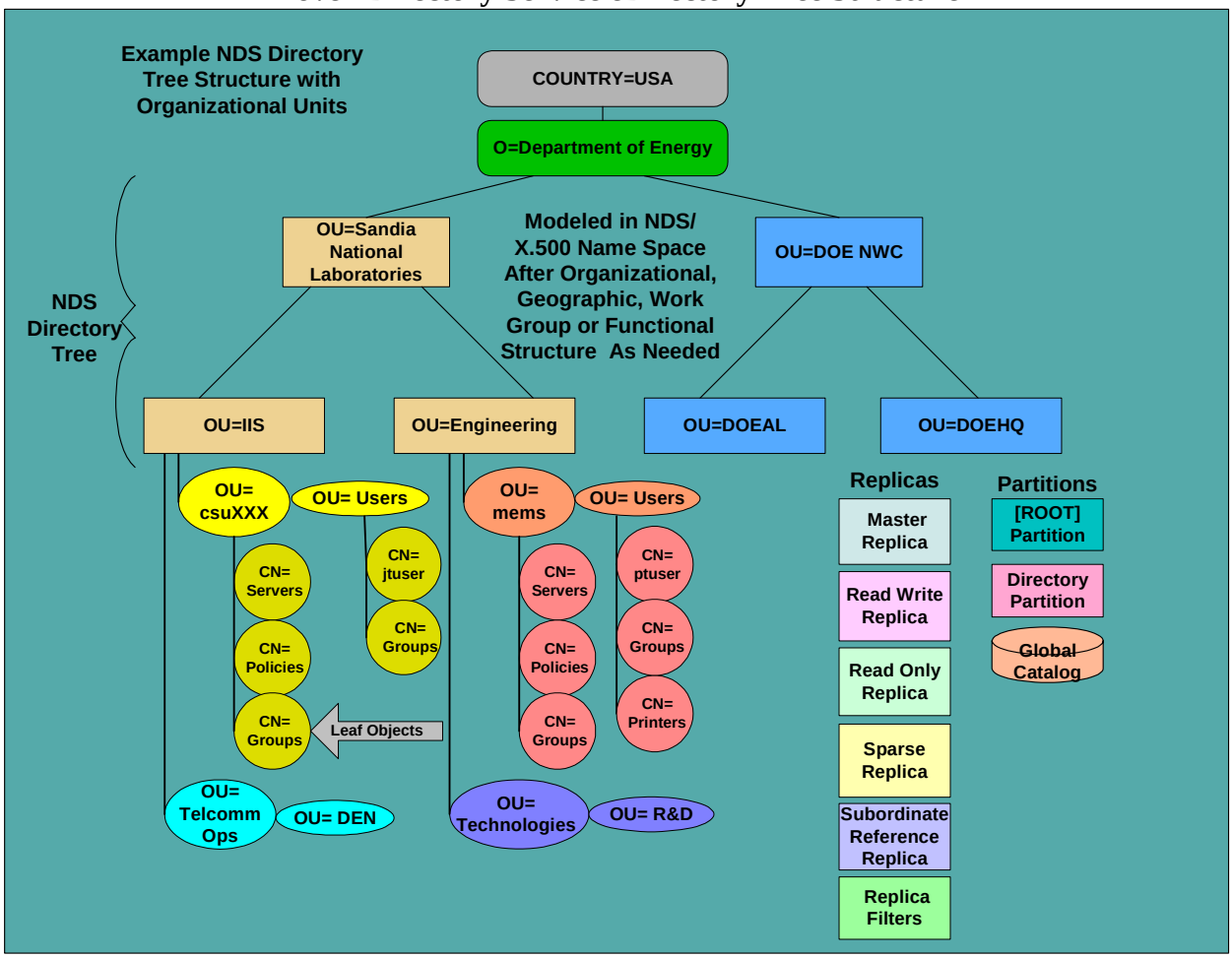

Figure 6

Sun/Netscape Alliance Directory Server

The Sun/Netscape Directory Server is a Lightweight Directory Access Protocol (LDAP) compliant X.500 directory service product. LDAP directory servers typically provide a directory structure for managing account access for distributed web-based resources and messaging.

X.500 Directory Tree Structure

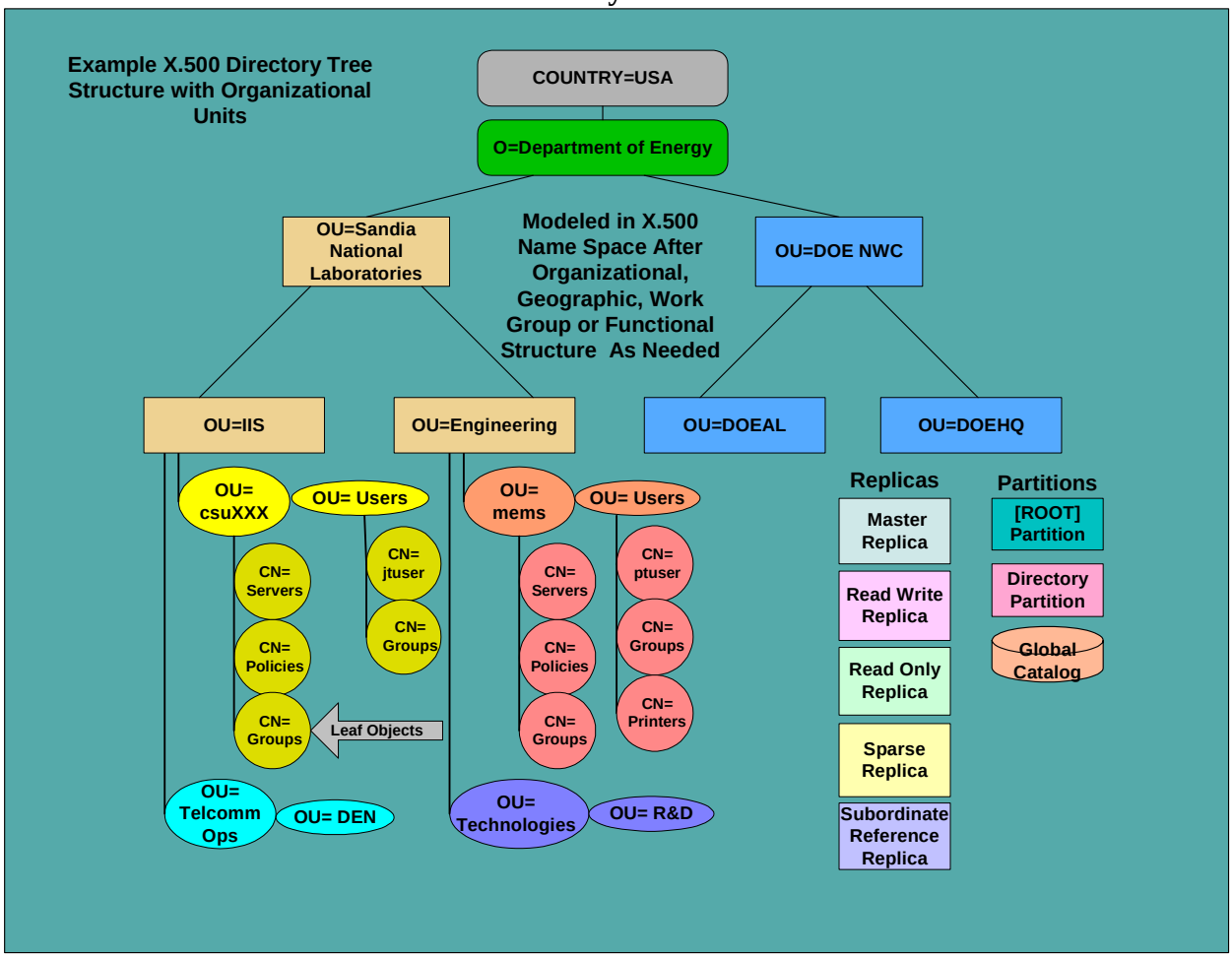

Figure 7

Directory-Service Naming

Directory-services naming can be a bit confusing. X.500 naming differs from the Lightweight Directory Access Protocol naming which differs from Active Directory naming. Consider that directory services are a hierarchical, distributed name space. The context of a common name (CN) leaf object is relative to its location in the tree. In a unified-directory environment common naming strategies can ease directory administration. The names should be short to alleviate tedious naming when referring to distinguished names or relative-distinguished names. The examples provided briefly illustrate the various name formats.

Standard Name Types:

- C=Country
- L=Locality
- O=Organization
- DC=Domain Component
- OU=Organizational Unit
- CN=Common Name

Standard Name Categories:

- Fully Qualified Domain Name - DNS name specifying a complete set of values with a terminating root delimiter (.).
  Example:
  ahost@sandia.gov.

- Relative-Domain Name - A DNS domain name that does not end in a terminating root delimiter.
  Example:
  ahost@sandia.gov

- Distinguished Name - A combination of an object's common name and its context. See examples below.

- Relative-Distinguished Name - The path of an object relative to the current context. See examples below.

- Common Name - A leaf objects' common name denotes an object within its context. See examples below.

Directory Information-Tree Context:
Context is an object's position in the directory tree. Listing the container objects from the object to the root of the directory tree specifies context.
Example:
OU=csu880, OU=snlnm, O=sandia

The Distinguished name of an object is a combination of its common name and its context.
Example:
CN=jtuser, OU=csu880, OU= snlnm, O=sandia

The Relative-Distinguished name is the path relative to the current context.
Example:
If the current context is:
OU=csu880, OU= snlnm, O=sandia
The then the relative-distinguished name for CN=jtuser, OU=csu880, OU= snlnm, O=sandia is CN=jtuser

X.500 Naming[1]
The name delimiter for X.500 naming is the comma (,).
Example:
O= snlnm, OU=csu880, CN=jtuser

Lightweight Directory Access Protocol Naming
The name delimiter for LDAP naming is the comma (,).
Example:
CN=jtuser, OU=csu880, O=Sandia, C=US

Active Directory-Service Naming
The name delimiter for active-directory naming is the comma (,). NetBIOS/UNC naming is supported for backward compatibility with Microsoft Windows NT. Active Directory supports Lightweight Directory Access Protocol naming for directory queries.
Example:
CN=jtuser, OU=csu880, DC=sandia, DC=gov

User Principal Names
Example:
Jtuser@sandia.gov

Novell Directory-Service Naming
The name delimiter for Novell Directory Service naming is the period (.). Novell Directory Service supports Lightweight Directory Access Protocol naming for directory queries.
Example:
CN=jtuser. OU=csu880.O= snlnm. C=US

The NDS Distinguished name of an object is a combination of its common name and its context proceeded by a period (.).
Example:
.CN=jtuser.OU= snlnm.O=sandia

Name Representation:
Typeful-Naming - Name representation indication object types.
Typeless-Naming - Name representation omitting object types.

Typeful-Naming
Example:
.CN=jtuser.OU=csu880.OU= snlnm.O=sandia

Typeless-Naming (analogous to DNS naming)
Example:
.jtuser.csu880.snlnm.sandia

Distributed Computing Environment (DCE) Naming
DCE Cells interact through an X.500 Global Directory Service (GDS) or DNS naming prefix.

[1] Note that X.500 naming differs from LDAP or other directory naming in that orientation is opposite of LDAP.

DIRECTORY-SERVICE INTEGRATION

The tools available to integrate disparate directory service products ease the integration burden where multiple vendor directories are deployed. Data replication and common-data representation are two means of maintaining symmetry with multiple directories.

MetaDirectories

Metadirectories are directory information-exchange tools that provide a method to integrate multiple directory services by collecting and sharing information among disparate directory structures. Stand-alone metadirectories can serve as migration tools but fall short of a long-term integrated directory-service solution. Microsoft has acquired ZOOMIT for Zoomit Via metadirectory technology, and Novell has integrated DirXML with Novell Directory Services eDirectory. Other metadirectory products available include Worldtalk Corp. Netjunction.

eXtensible Markup Language (XML)

The eXtensible Markup Language, a subset of the Standardized Generalized Markup Language (SGML), is a universal standard for representing structured data in heterogeneous environments.

XML defines web data elements for business-to-business documents and the element contents. For example, the developer can define data items that represent product, sales rep and amount due. This allows web pages to function like database records. By providing a common method for identifying data, XML supports business-to-business transactions and is expected to become the dominant format for electronic data interchange.

- XSL - Extensible Stylesheet Language.
- XSLT - XSL transformations.
- XLink - Rules for hyperlinks in an XML document.
- XLL - Previous name for XLink
- XPointer - Rules for linking to an XML document.
- XPath - Rules for addressing internal elements.

Note: XML statements define data content, whereas the HTML lines deal with fonts and boldface. XML defines "what it is," and HTML defines "how it looks."

Directory-Services Markup Language

Bowstreet Software developed the Directory-Services Markup Language in conjunction with the DSML Working Group. Directory-Services Markup Language is a set of XML tags that defines the contents of a directory and allows multiple directories to exchange information. The Directory-Services Markup Language provides a common format for directory-access protocol query results.

Novell Directory eXtensible Markup Language

Novell DirXML is directory-interchange software that integrates Novell Directory Services with other directories including Exchange, Lotus Notes, Microsoft Active Directory and others. It provides agents that monitor the activity in the directories and uses XML to exchange the updated data. DirXML functions to synchronization disparate directories as a metadirectory tool.

Novell DirXML is a Metadirectory Tool for Multi-Directory Synchronization

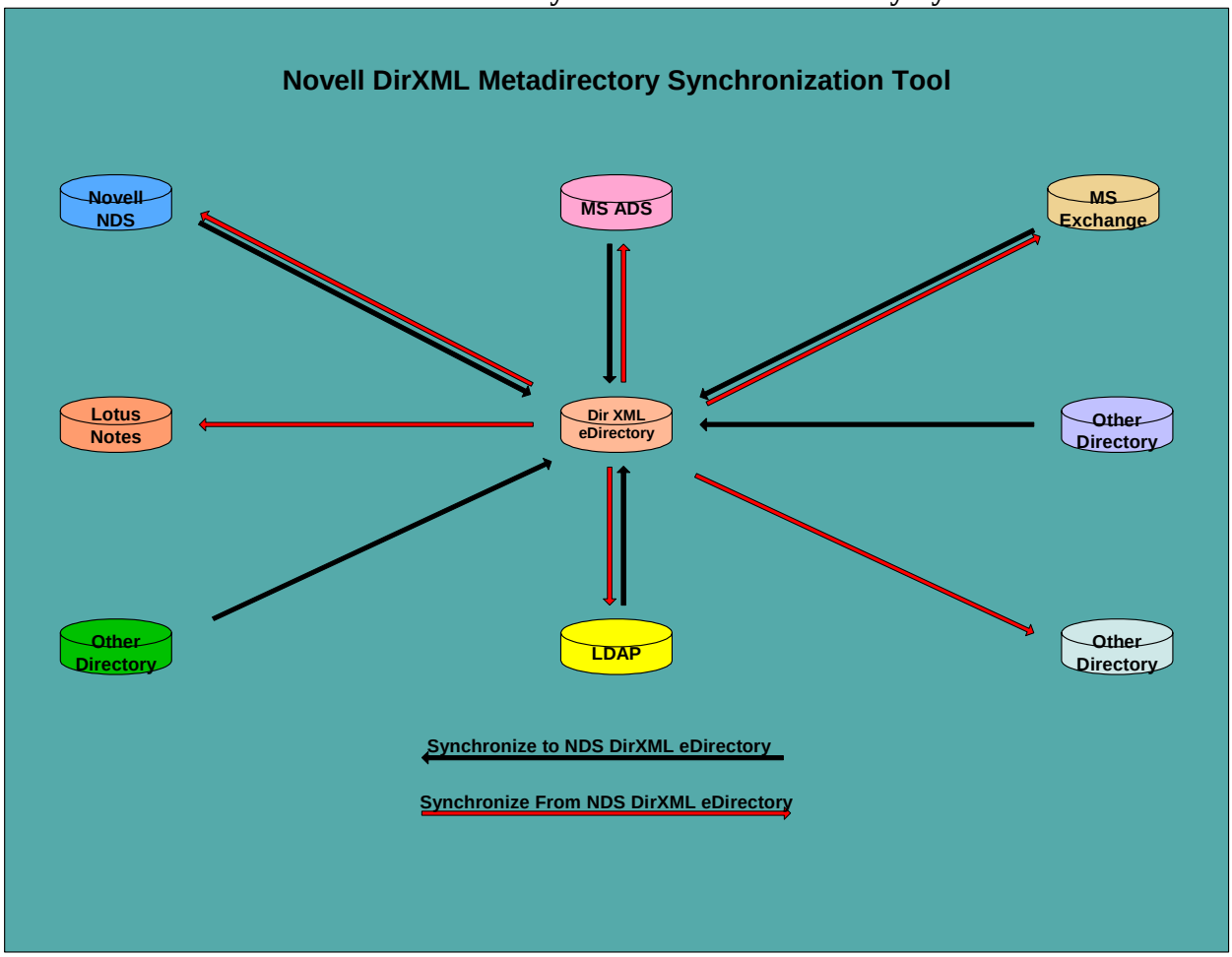

Figure 8

NETWORK MANAGEMENT AND POLICY-BASED NETWORKING

The Distributed Management Task Force (DMTF)

The DMTF was originally founded as the Desktop Management Task Force in 1992 and was renamed the Distributed Management Task Force in 1999. The following is a brief list of the Distributed Management Task Force accomplishments:

- Web Based Enterprise Management specification
- Directory Enabled Networks specification
- eXtensible Markup Language (XML) / Common-Information-Model
- CIM 2.1 specification
- CIM 2.2 schema
- CIM 2.3 user-security model
- CIM 2.4 policy and network models
  - Quality of Service and IPSec sub models
- HyperText Transfer Protocol (HTTP) Mapping 1.0

Current network management implementations are device centric. The Directory-Enabled Networks and Common Information Model specifications enhance TCP/IP based service provision protocols such as the ReSource reserVation Protocol (RSVP) and network management protocols such as the Simple Network Management Protocol (SNMP). The Directory-Enabled Networks and Common Information Model specifications allow for a managed network based on the relationship between applications and:

- Network devices
- Network services
- Network resources

Policy-based networking leverages the aggregate association of logical objects to apply security and control rules for access, management and security of network services and resources.

The Distributed Management Task Force Common Information Model

The Common Information Model specification provides for a standard information model to model network elements or components in sufficient customizable detail. The information model defines:

- Profiles and policies
- Devices, protocols and services

This allows leveraging the directory for integration of users, applications, and network services in an extensible service-oriented framework.

The Directory-Enabled Networks and Common Information Model Specifications Permit Embedded Intelligence

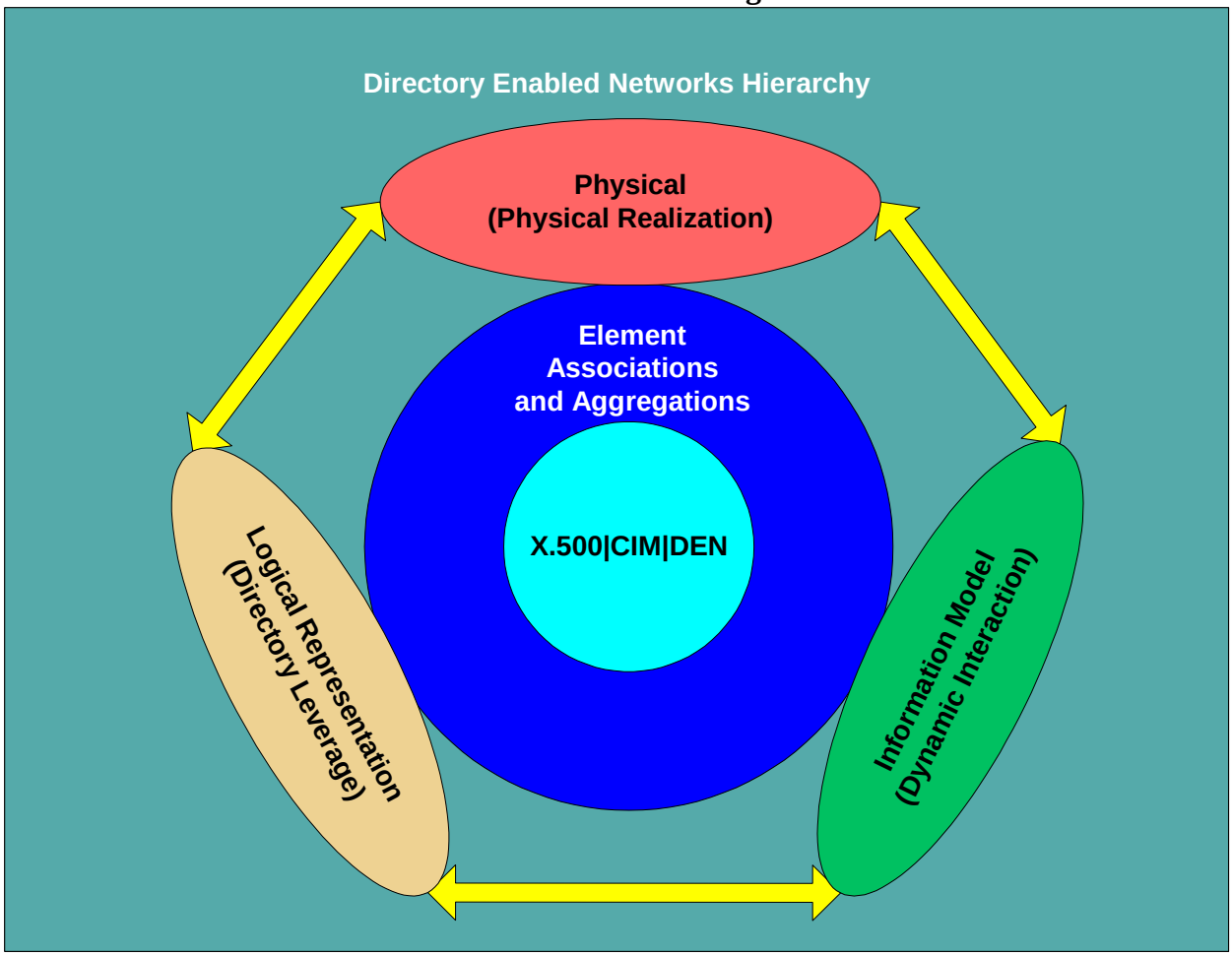

Figure 9

Network elements are inherently more complicated than static directory objects and must be dynamic to model the interaction between:

- Network elements
- Network services
- Network clients - applications and users

Policy-based network management requires a network-wide model as opposed to a device-centric model. The Directory-Enabled Networks and Common Information Model specifications present the methodology to allocate network resources based on business rules and network conditions. Policy-based networking can be effectively used for Quality of Service, Voice and other active applications.

A point of clarification: Directory-Enabled Networks (DEN) is an industry specification; Directory Enabled Networking is a design philosophy.

The Distributed Management Task Force Directory-Enabled Networks Specification

The Directory-Enabled Networks (DEN) specification is an extension to the Common Information Model specification. Directory-enabled network services permit enfranchisement of network elements by overlaying embedded intelligence across the network. This embedded intelligence utilizes the relationships or associations and aggregations of logical objects to actively manage the network. Policy-based networking enables the management of the network as a whole instead of managing individual network elements.

Distributed Management Task Force goals for the DEN specification:

- Model network elements and services, and their interaction with other network elements, in a managed system
- Provide means for interoperable network-enabled solutions
- Enable applications to leverage the power of the network without requiring the user to know or configure network-related information.
- Define a way to manage the network, not individual elements or devices in the network.

The DEN specification is composed of the following hierarchy:

- CIM 2.1 specification
- CIM 2.2 schema
- CIM 2.3 user-security model
- CIM 2.4 policy and network models
    - Quality of Service and IPSec sub models

The Directory-Enabled Networks Specification is an Information Model to Directory Map

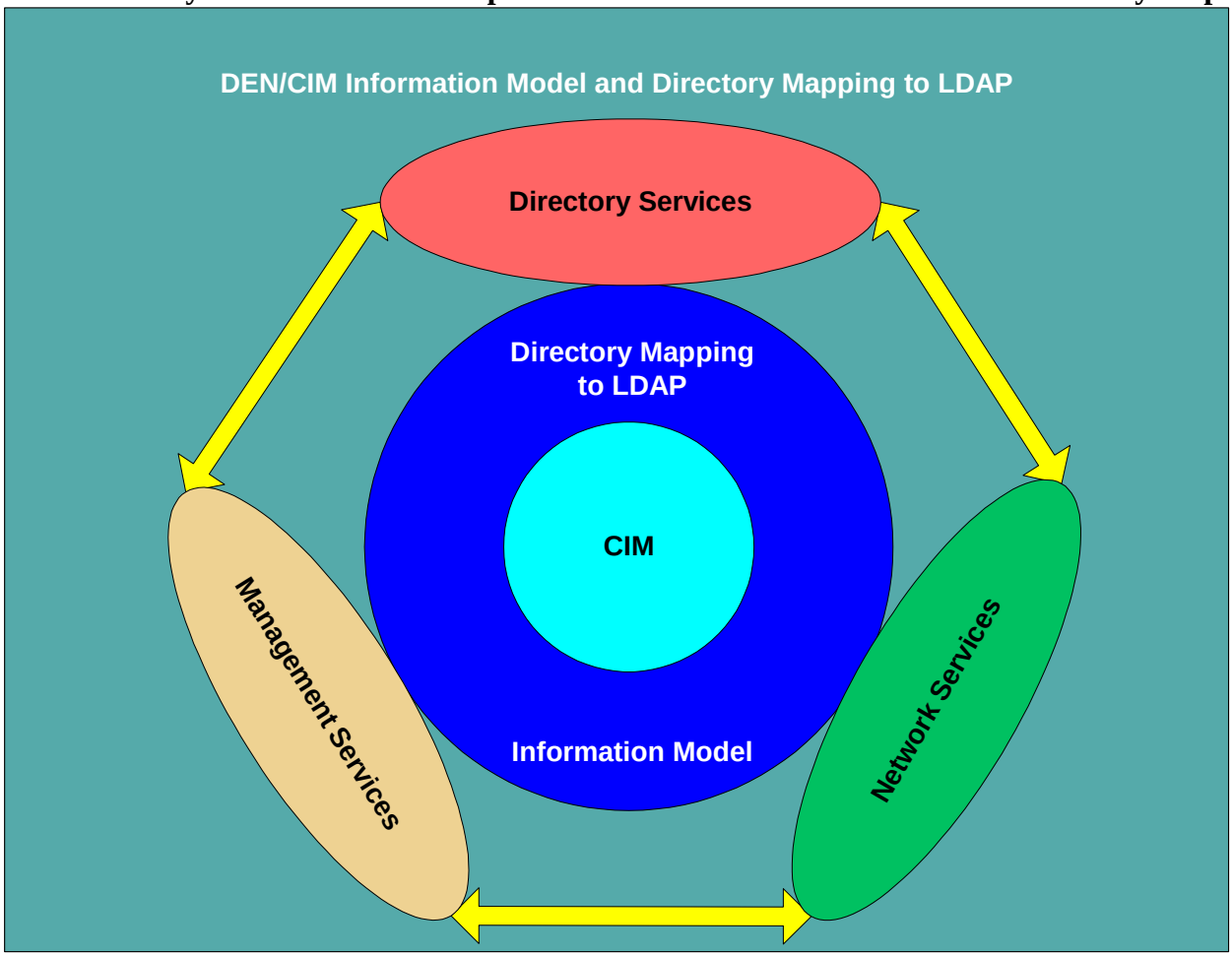

Figure 10

The DMTF Web-Based Enterprise Management (WBEM) group and the IETF Policy Framework Working group are cooperating in the development of directory standards. Microsoft NT & Windows 2000, Sun Solaris 8 and Novell NDS support the DMTF Common Information Model (CIM). CIM, as a definition of an information model can be mapped to the Common Management Information Protocol (CMIP), Common Object Model (COM), Common Object Request Broker Architecture (CORBA) or other data formats.

The IETF Policy Framework Working group levels of abstraction (Domain, Mechanism, Implementation Specific and Instance Specific), DiffServ (Differentiated Services), Common Open Policy Service (COPS), SNMP, and SNMPConf (SNMP Configuration MIB) in conjunction with the DMTF CIM, WBEM and DEN specifications offer integrated overall management and quality of service.

Directory-enabled network installations are on the threshold of tomorrow's technologies. Cisco Systems Cisco Networking Services (CNS), Cisco Architecture for Voice, Video and Integrated Data (AVVID) and Quality Policy Manager products include directory-services functionality. As directory-enabled networks become prevalent in the industry, new devices will have the capability to communicate via the Simple Network Management Protocol and the Lightweight Directory Access Protocol.

Directory-Enabled Networks object classes include:

- Physical package
- Network element
- Network services
- Application
- System
- Profile - associated with the user , group or Organizational Unit
- Support for vendor-specific subclasses

The benefits of implementing the Directory-Enabled Networks and the Common Information Model specifications in a directory-enabled environment include:

- Embedded intelligence.
- Method to manage increasing configuration complexity of network devices.
- Method to ensure consistent policies are applied to network elements.
- Method to enable applications to be associated with network services.
- Means to ensure mission-critical applications have the priority to guarantee service.
- Method to link business processes and requirements to network elements
- Services associated with clients enabling multiple services to realize a single function.

The Internet Engineering Task Force has several drafts in development that tightly integrate with the Directory-Enabled Networks specification. Cisco policy-based-networking product strategies are based on the Directory-Enabled Networks specification. With the industry momentum building for directory-enabled networking, a wave of directory enabled products will be released in the coming year.

The Policy Framework Working Group (PFWG)

The Policy Framework Working Group is endeavoring to define a framework for a multi-vendor architecture sustaining a heterogeneous policy domain. This includes a vendor- independent and device-independent policy-description language and schema based on the Directory-Enabled Networks specification object classes that define a common representation of policy information.

The following illustration depicts the network service environments of Sandia National Laboratories with a heterogeneous directory-service emphasis represented just under the business process layer.

Sandia Heterogeneous Directory Enabled Network Environment

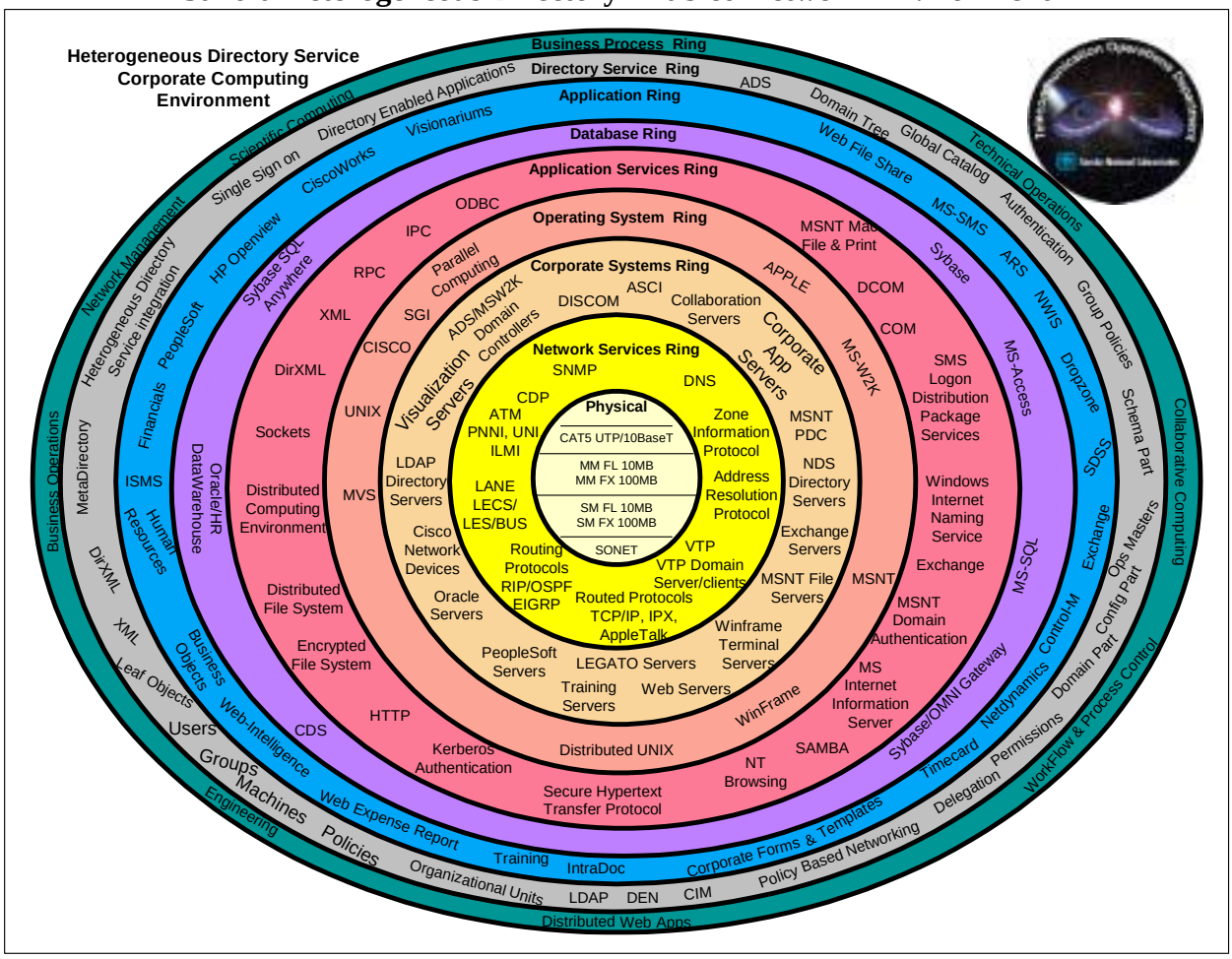

Figure 11

The difference in the Sandia heterogeneous directory-enabled network environment and the Sandia Active-Directory-enabled environment is standards-based support for multiple computing platforms.

DIRECTORY SERVICE PROJECT DESIGN GUIDELINES

Careful planning and coordinated effort is required for an enterprise directory service project. Typically a large network-computing enterprise is heterogeneous in nature supporting multiple computing platforms as required by complex customer environments. Integration issues are exacerbated when considering a multiple-organization directory-service project. Large enterprise networks will likely integrate multiple directory service products.

The following illustration depicts a heterogeneous unified multi-directory environment.

Unified Directory Service Solution

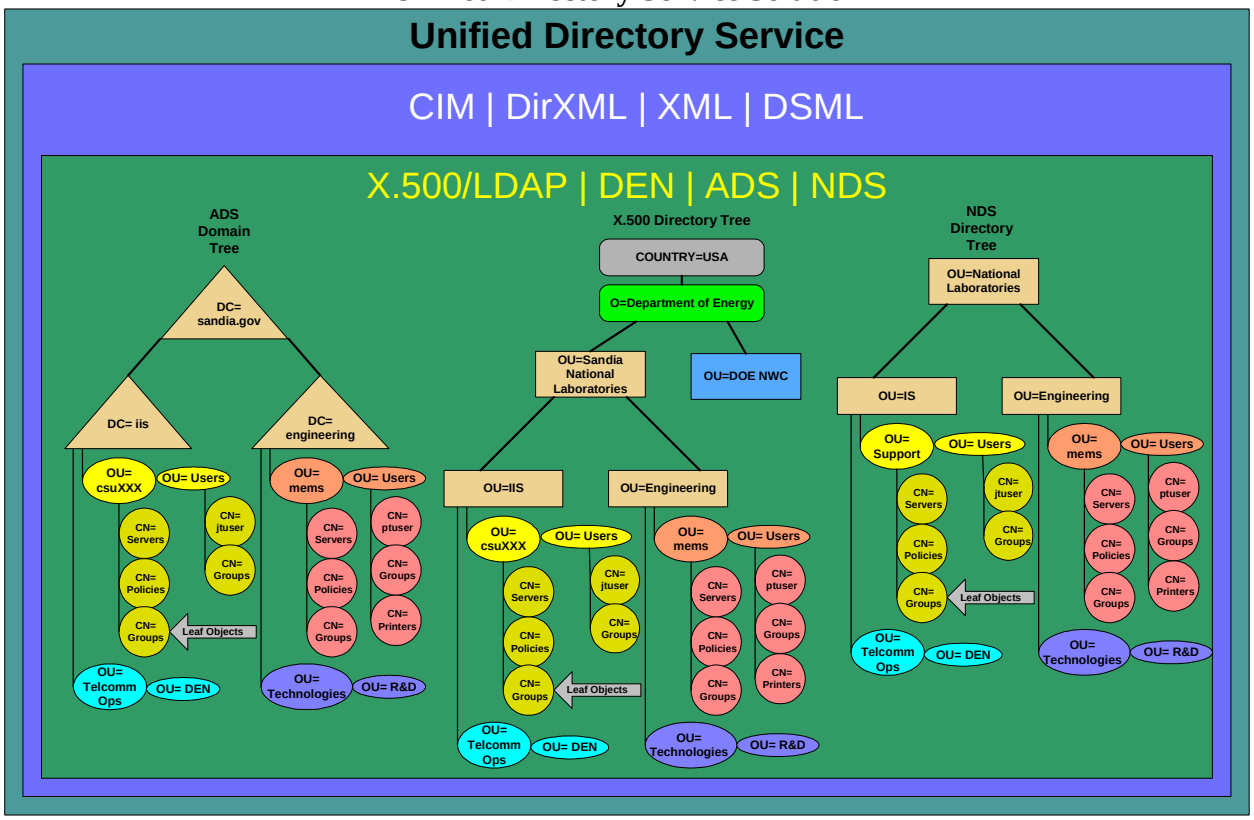

Figure 12

Industry Standards Based Design

An industry standard-based directory-design approach and common-design methods such as a common naming convention, facilitate enterprise directory scalability and directory interoperation. A standards-based directory design should be pursued to ensure multiple vendor directory interoperation in a large network-computing environment.

Figure 13 depicts a brief representation of the design considerations for a DOE NWC unified multi-organizational project.

Unified Directory Design Considerations

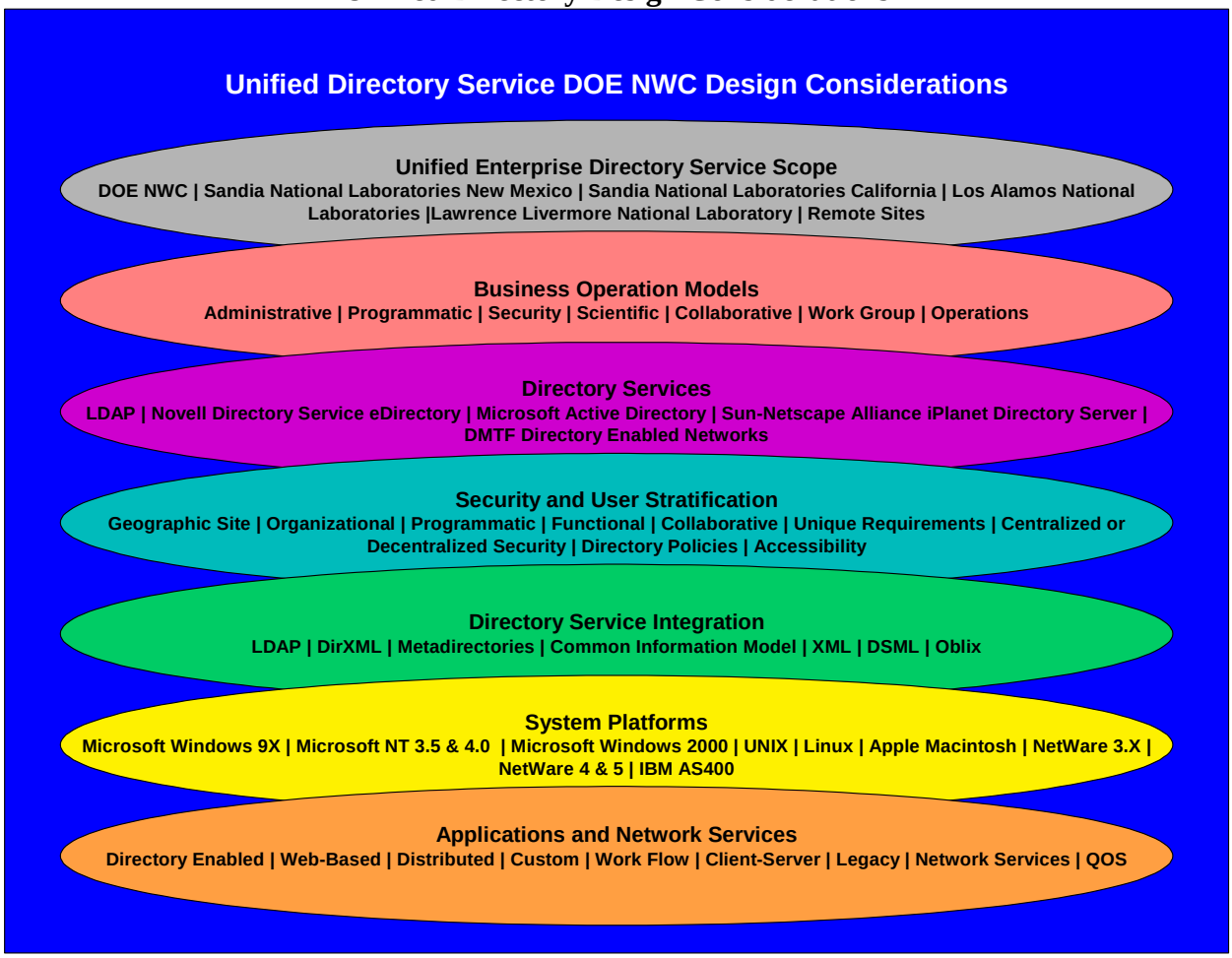

Figure 13

The complexities presented when addressing a DOE NWC unified directory-service architecture pose significant challenge. The systems engineering approach should comply with industry best practices such as the ISO 9000 recommended standards. This would include an evaluation of available products for feature and function, and controlled change management and design processes.

International Standards Organization Design Guidelines

The ISO 9000 quality system defines best practice business-process elements. The Sandia National Laboratories Telecommunication Operations department has adopted the ISO 9000 methodology and has defined nine processes that apply to the network services business. These processes are:

- Orientation and Training Process - OTP
- Continuous Improvement Process - CIP
- Organizational Communication Process - OCP
- Trouble Resolution Process - TRP
- Asset Management Process - AMP
- Document Management Process - DMP
- Development & Evaluation Process - DEP
- Change Management Process - CMP
- Network Management Process - NMP

The Development & Evaluation Process and the Change Management Process are well suited to ensure the integrity of the evaluation and design stages of a large directory-service design. These processes are presented as a model for maintaining the quality and rectitude of a complex design project.

ISO 9000 Telecommunication Operations Change Management Design Process

Sandia Telecommunication Operations ISO 9000 Network Design Change Management Process
Telecommunication Operations Department Manager - Michael Sjulin
Bruce C. Whittet, Process Owner, June 5, 2000

Flowchart of the Change Management Process

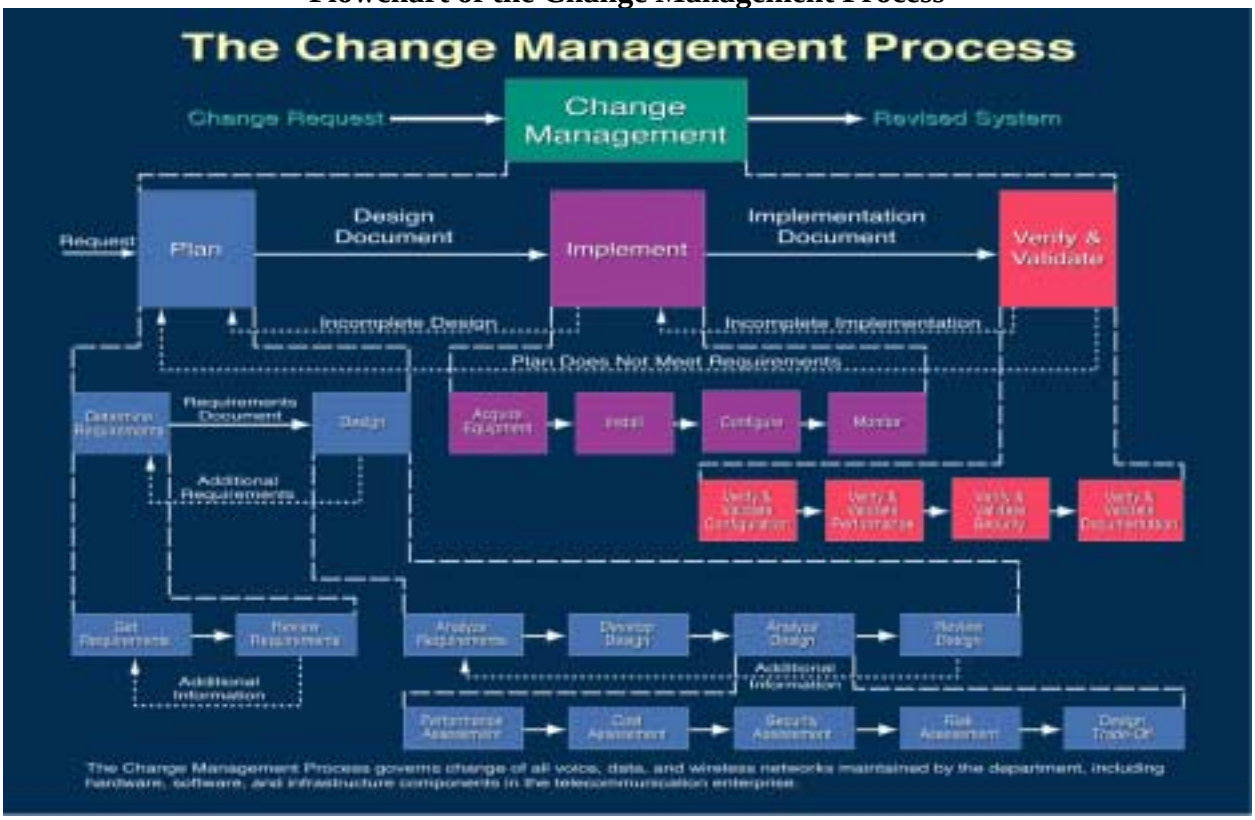

Figure 14

ISO 9000 Telecommunication Operations Design/Evaluation/Development Process

Sandia Telecommunication Operations ISO 9000 Design/Evaluation/Development Process
Telecommunication Operations Department Manager - Michael Sjulin
Pat Manke - Process Owner, May 19, 2000

Flowchart of the Design/Evaluation/Development Process

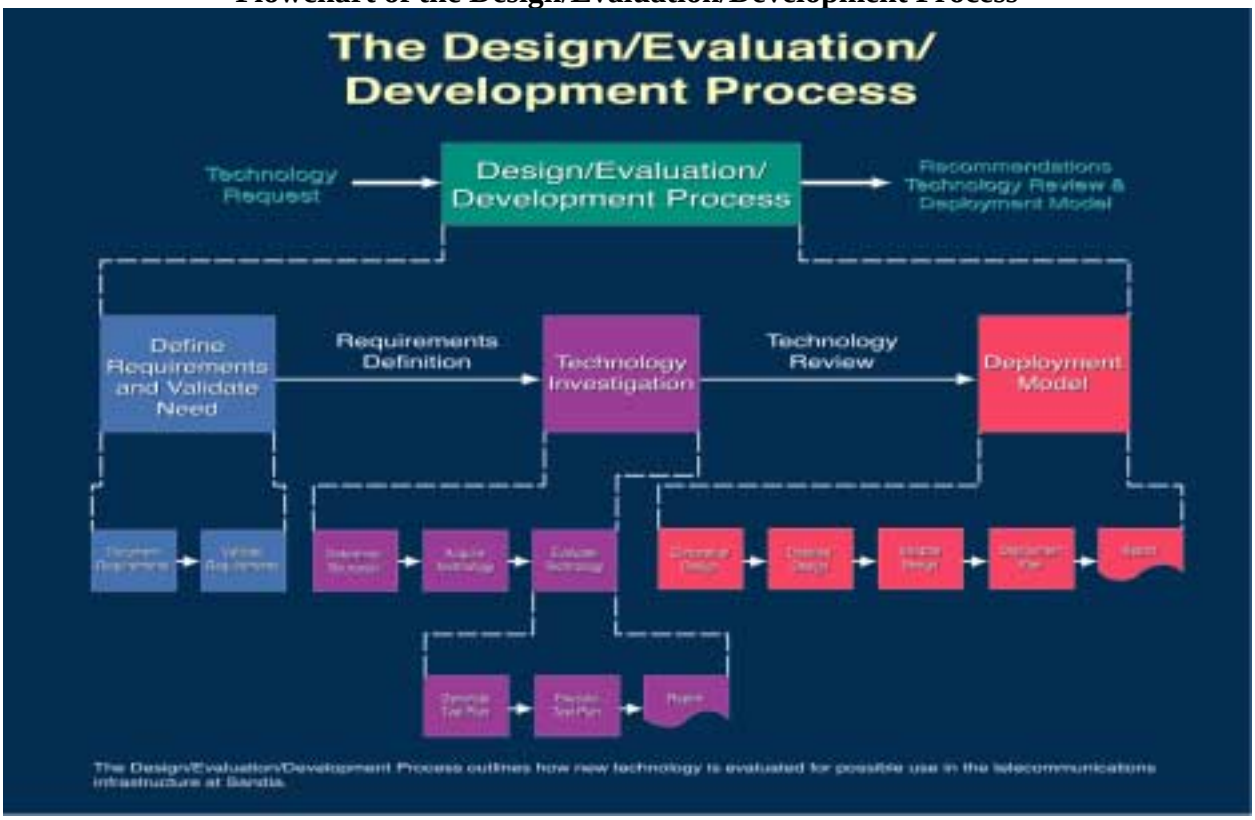

Figure 15

Test and Evaluation

The planning phase of a directory-service design project requires an adequate test environment for evaluation of directory-service products. The test environment also serves to evaluate implementation and migration strategies.

Sandia National Laboratories Enterprise Test Network

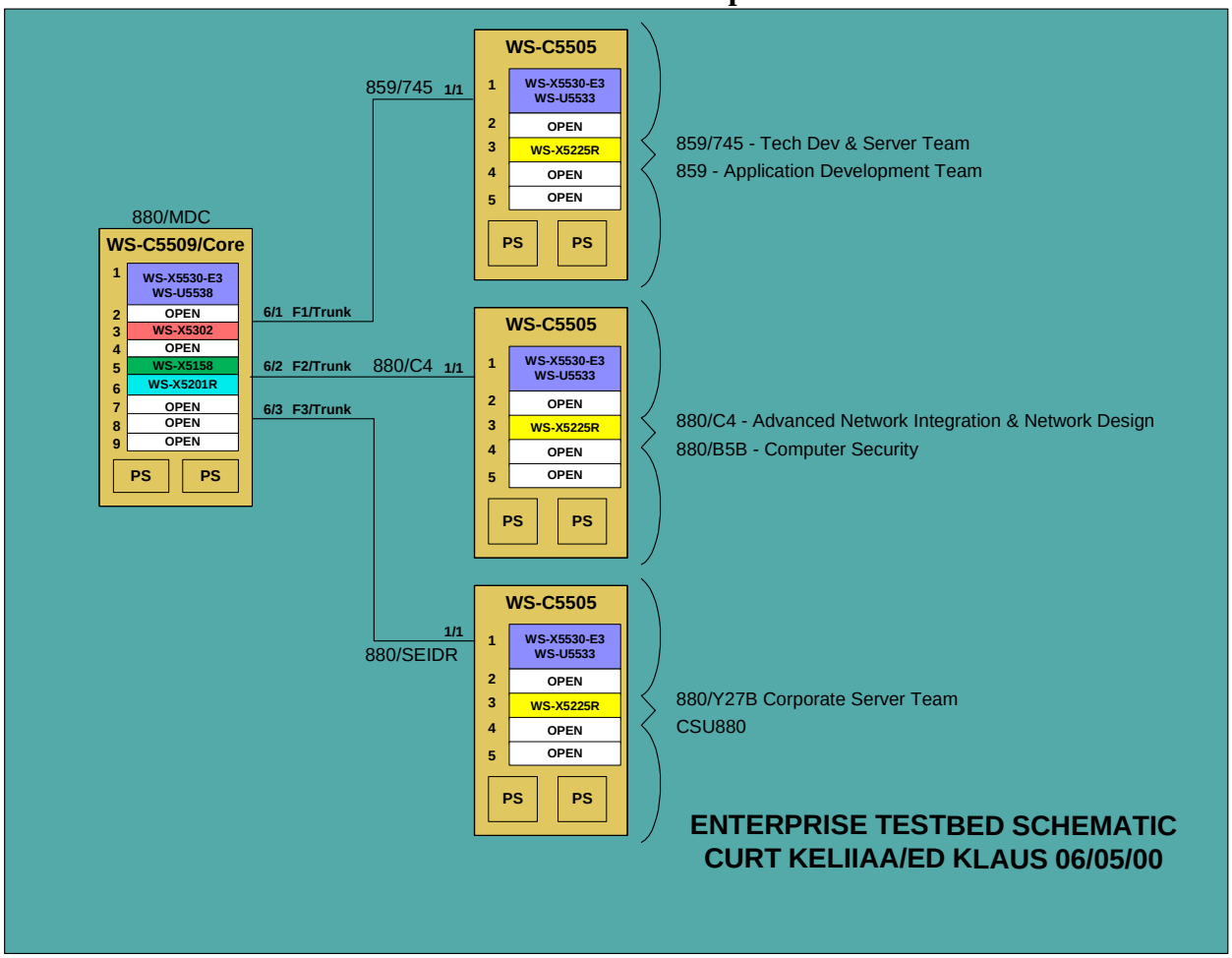

Figure 16

Illustrated is the proposed Sandia Enterprise Test Network. This network would allow an unprecedented network-computing test environment for Sandia National Laboratories. This illustration depicts the Cisco infrastructure environment that would allow for a site (set of well-connected networks) level evaluation.

A broader computing environment with network services and client-server hosts would be required for evaluating directory-enabled applications. An application review policy should be put in place for directory-enabled application evaluation and to investigate legacy application support issues.

Directory Services Design and Implementation Project Outline

Project Approach
Project Team
Project Manager
Computing interests represented
Business operations interests represented
Software development interests represented
Technical assignments
Project Scope
Complexity analysis
Interoperability matrix
Project Goals
Project schedule
Mission; Motivation; Justification
Project Requirements
Operational
Functional
Administrative
Training
Resources
Corporate Information
Geography
Contacts
State of The Network definition
Business processes interdependencies
Operations and operational interdependencies
Audit current infrastructure technologies and identify project constraints
OSI Layers
Application
Presentation
Session
Transport
Network
Data Link
Physical
Wan Layout
High/Low speed WAN requirements
Slow link replication schedules
Identify, Quantify and Prioritize Application usage
Planning Phase
Identify and Evaluate Available Solutions
Evaluation network
Product comparisons
Product evaluations
Evaluation report
Strategic decision
Migration Plan
Migration goals
Migration strategy
Migration issues
Migration schedule
Migration milestones

Design Phase
Services Distribution Plan
Network service distribution map
Network service accessibility guidelines
Service provisioning
Quality of Service
Directory Information Tree Design
Administrative model
Operational, Organizational and Geographic model for tree structure
Administrative accessibility guidelines
DNS for ADS
Integrated DNS and DHCP (ADS & NDS)
Define naming standards
Schema and Directory System Agent (DSA) design
Partition & Replication topology
Modeling
Traffic characteristics
Accessibility plan
User stratification
Administrative jurisdiction
User accessibility requirements (7X24)
Applications
Application Profiles
Application usage detail
Legacy application compatibility
Distributed application system dependency matrix
Directory enabled application integration plan
Security Plan
Security configuration guidelines for servers and workstations
Layered security integration plan
Administration model
Centralized
Decentralized
Policy architecture
User and Group policies
Security, Access & Authentication policies
Network service policies
Administration policy
Policy accessibility guidelines
Policy to authority maps
Implementation Plan
Network Management Plan
Common information model
Network management tools
Design Review
Conceptual design review
Interim design review
Final design review
Implementation Phase
Implementation to plan
Maintenance and Continuous Improvement Phase
Audit, Evaluate & Improve

Active Directory Service Accessibility Guidelines

Example ADS Accessibility Guidelines	
Topic	**Standard**
Domains	The domain is the smallest unit of partitioning Exception to Transitive Trusts - Domain Explicit Trusts
Administrative Model	Administrative Jurisdiction Enterprise Admins Domain Admins Schema Admins Administrative Delegation Centralized Administration Decentralized Administration
Organizational Unit	The OU is the smallest unit of authentication
Group objects	Use group objects only when all group members exist in the same physical location. Each group can have two scopes, distribution and security. Security groups support Access Control Lists, Distribution groups do not. Only security groups are outlined in this example. Mixed Mode: Domain Local Security Groups - Can contain domain global security and distribution groups and domain local and universal distribution groups. Domain Global Security Groups - can contain no other security groups, only users. Universal Security Groups - Universal security groups are not available in Mixed Mode. Native Mode: Domain Local Security Groups - Can contain domain local, domain global and universal security and distribution groups. Domain Global Security Groups - can contain domain global security and domain local distribution groups. Universal Security Groups - Universal groups are held in the Global Catalog. Only available in Native Mode. Universal Security Groups can contain domain global and universal distribution and security groups.
Policies	Group Policies Group Policies - Group Policy Object - Published & Assigned Local System Policies
Profiles	Use Profile objects when user objects need to access to network resources.

Example ADS Accessibility Guidelines	
Topic	**Standard**
Rights and Permissions	Security Descriptor - Defines Access & Permissions ADS Permissions Full Control Read Write Advanced Object Type Extended Permissions Inheritance Inheritance Blocking Inheritance Override Discretionary ACL Defaults for Authenticated Users - Read Defaults for Administrators - Read | Write | Create ACL Defaults for Domain Administrators - Full Control | Read | Write | CACL Defaults for Enterprise Administrators (Inherited) - Full Control | Read | Write | CACL
Login scripts	MMC - Windows Settings Logon & Logoff Scripts Specified to run synchronously or asynchronously in the User Configuration Administrative Templates section of the Group Policy Object.
Access Control Lists	Create ACL permission Discretionary ACL System ACL - Auditing
Active Directory Design Notes:	
Active Directory is modeled after DNS. The DNS namespace should be in place prior to installing the first Active Directory domain.	
Map administrative delegation roles to Authority.	
Cannot rename ADS Root without reinstall.	
No recovery if all or only Root Domain Controller is lost.	
Operations masters should be only Domain Controllers the are at the Root Domain (sandia.gov)	
Accommodate distinct DNS names to use multiple Directory Trees	

Novell Directory Services Accessibility Guidelines

Example NDS Accessibility Guidelines	
Topic	**Standard**
Group objects	Use group objects only when all group members exist in the same physical location.
Profile objects	Use Profile objects when user objects needing access to network resources exist in more than one container. For example, to grant members of an organization that spans CSU boundaries access to common network resources.
Organizational Role objects for network administrators note: This document requires further review for compliance to the Novell security model.	Create an organizational role object at certain levels with two members: the network administrator and the backup administrator. There are five administrator role levels defined. level 0, 1, 3, 4, and 5. Level 2 is not implemented. Level 0 - Admin, all rights starting at [ROOT]. Controlled by an organizational role in a hidden directory tree security area. Occupants - enterprise wide administrators. Level 1 - Container Admin, No object rights to anything else in the container, cannot change ,add or remove users from this role. Can install servers but cannot perform partition operations. All file system rights to volumes and servers in the container. Controlled by an organizational role in Customer Service Unit (CSU) containers throughout the tree. Occupants - server managers. Level 3 - Container Admin, All rights within a container except CREATE and RENAME (can modify existing objects: passwords, group memberships, and login scripts. Cannot partition or install servers. All file system rights to the PUBLIC, APPS, USERS directories. Controlled by an organizational role in CSU containers throughout the tree. Occupants - network administrators. Level 4 - Container Admin, Limited property rights for user objects. No rights to create or rename objects. No rights to partition or install servers. No file system rights. Controlled by an organizational role in CSU containers where such management is needed. Occupants - help desk personnel. Level 5 - Container Admin, This is a special level for corporate application controlled servers. Minimal rights to NDS objects, ability to assign group memberships, change passwords and login scripts. Cannot create objects, add or remove users to this role, or partition and install servers. All file system rights. Controlled by an organizational role in containers where such management is needed. Occupants - corporate application administrators. Organizational role membership - should be controlled by level 0 or level 3 administrators. NDS can be designed for centralized administration or decentralized administration. Decentralized administration is recommended for the CSU environment.

Example NDS Accessibility Guidelines	
Topic	**Standard**
Inherited Rights Filters (IRF) for containers	NDS rights may be blocked by use of IRFs at the container level to create secure containers. If the SUPERVISOR right is blocked and the container admin user is deleted or has SUPERVISOR rights removed there is a danger of creating an administrative black hole. The following organizational role can be set up to protect against this occurrence. Create a secure hidden container. Create an admin organizational role with SUPERVISOR NDS rights. The container admin user object and the backup up admin object should be granted SUPERVISOR rights and also be added to the organizational role. In the event that the container admin user object loses SUPERVISOR rights the organizational role membership retains those rights.
Application directories and drive mappings	Standard directories should follow the CSU standard. i.e. M:=\\Servername\POdirectory, I:=\\Servername\Sandia, Q: \\Servername\SYBASE Recommended home directory is H:=\\Servername\users\%home directory.
Directory Map objects	Directory Map objects should be created for shared applications running on Novell 5.X Directory Map objects can be referenced in the login script(s) for standard drive mapping. If the application location or directory name changes the Directory Map object property can be changed without need to change the login scripts. This allows one change with global effect.
Login scripts	Container login scripts should be used to set the environment for all users and groups with the container. This would include common drive mappings, access to printers and print queues, and server attachments to Microsoft NT FPNW servers. (Eventually FPNW should be removed from the network.) Create Profile login scripts when user objects needing access exist in more than one container. If multiple profile login scripts are to be used within a single container then CSU profile standards should be established that define the types of profile objects that may be used. (For example, network administrators, server managers, postmasters, network communications specialists, desktop service representatives, and SNL organizational needs.) Members of differing groups may be granted access within a single profile login script using the “IF MEMBER OF” statement to specify access by group membership. Profile login scripts add an additional level of administration over container login scripts. User login scripts should only be used when required. Individual needs can be met within the container login script using the %login_name identifier variable. Mobile users can be accommodated in the login scripts using the %HOME DIRECTORY, %FILE_SERVER, and %NETWORK identifier variables.

Example NDS Accessibility Guidelines	
Topic	**Standard**
User menus	User menus should not be required for Sandia.
Alias objects	Alias objects should be used for physical network resources. Aliasing an NDS object is convenient for providing access to network resources located in another part of the directory tree.
Bindery context	Bindery context for each server should be set at the servers' container level.
Security precautions	The SUPERVISOR NDS right should not be granted to server objects because the SUPERVISOR right is inherited by file system.
Sandia National Laboratories Environment Considerations	Eventually Microsoft Gateway Service for NetWare (GSNW), and Microsoft File and Print services for NetWare (FPNW) should be removed from the network. GSNW and FPNW were intended to be transitional products. A client based configuration could be implemented to access Novell network resources and Microsoft network resources without Network Operating System (NOS) emulation software. A testbed would need to be setup to determine the best client configuration for this purpose. Mixed environment connectivity might be accomplished with a multiple protocol stack client configuration until all clients are migrated to TCP/IP. At that time all network resources could be accessed through TCP/IP. For the current class of Intel based systems using Microsoft Windows 95 or Microsoft Windows NT Workstation the Novell client and the Microsoft client could be configured in a multiple protocol configuration. This would allow access to Novell resources via a Novell protocol stack and Microsoft resources via a Microsoft protocol stack. Macintosh clients are provided full NDS support through the Microsoft client for NDS (Novell Directory Services). There is also name space support and Apple File Protocol (AFP) support provided by both Novell and Microsoft. Third party Macintosh TCP/IP NDS clients are also available. TCP/IP, NFS (Network File System) and native NDS support provide UNIX and Linux clients access to Novell 5, X servers. Novell provides for an NT server object for NDS. Novell supports native TCP/IP.
NDS design Notes:	
Keep two or three replicas to a local site.	

Common Naming Convention

The successful integration of an enterprise directory-service solution that enfranchises disparate systems is dependent on common planning and implementation strategies. A common naming convention is needed to integrate disparate network name resolution methods and network directory services. Examples of common naming methods are provided in Appendices B, C & D as guidelines for defining a common naming convention. A Sandia common naming convention would enable a cross platform strategy to implement enterprise-information-governance. A common naming convention would facilitate systems management and integration by defining a common convention for various network-naming schemes and logical-network-object names as represented in an X.500 name space structure.

Multiple standard name formats should be supported including RFC822, HyperText Transfer Protocol Universal Resource Locator, Lightweight Directory Access Protocol Universal Resource Locator, X.500 and Microsoft Universal Naming Convention names. Internet, Intranet and Extranet web based applications, including Simple Mail Transfer Protocol email, could be integrated with the Lightweight Directory Access Protocol to enable an enterprise distributed-information-system.

At the time of this writing, Microsoft NT 4.0 is the Sandia Common Operating Environment (COE) network-operating system and consideration must be given for enterprise integration of the Microsoft Windows Internet Naming Service and the Domain Name System. A common naming convention will provide symmetry with Microsoft Windows Internet Naming Service and Domain Name System names. This will ease Domain Name System and Microsoft Windows Internet Naming Service enterprise network administration, and migration to Microsoft Window 2000.

Corporate applications such as the NetWork Information System and PeopleSoft could take advantage of directory services to provide shared, reliable access in the enterprise distributed-information system. Directory services will play a key role in the successful implementation of a location-independent enterprise distributed-information system. A common naming convention will provide the base in which disparate systems can integrate into an enterprise distributed-information system.

DIRECTORY SERVICES TECHNICAL DISCUSSION

Industry Direction

The industry standards bodies and major vendors are pursuing directory-enabled initiatives as the foundation for universal connectivity. Directory-based Sun/Netscape Alliance, Novell and Microsoft products are available today. Cisco is fast approaching these initiatives and has released limited directory-enabled products. Cisco Systems' Cisco Networking Services (CNS) policy-based networking strategy is founded on the Directory Enabled Networks (DEN) and the Common Information Model (CIM) specifications. The initial release of CNS is integrated with Microsoft Active Directory, CNS/AD. As other industry network equipment vendors adopt industry standards, secure multi-vendor dynamic service provision will become available.

The Internet Engineering Task Force (IETF) and the Distributed Management Task Force (DMTF) standards and specifications promise to further promote directory-enabled networks. The DMTF Directory-Enabled Networks and Common Information Model specifications define a consistent manner to represent physical, logical and policy network elements as logical objects. The industry IETF[2] and DMTF[3] standards and specifications provide the building blocks to build a comprehensive managed network. The DMTF Directory-Enabled Networks specification takes directory-service technologies beyond account and machine administration and into network device and dynamic-service management.

The associations of logical objects support the concept of policy-based networking. For example, a user or application is represented as a client of a network service with configuration and security constraints applied dynamically through a policy. This is in contrast to device-by-device negotiation for bandwidth with protocols such as the ReSource reserVation Protocol (RSVP). Directory-services, the information-model and policies allow for management of the network as a whole instead of as isolated elements. The industry adoption of directory-service technologies mandate that information technology providers evaluate information services from an enterprise perspective.

The Benefits of Directory Services

Directory-service benefits include improvement in computer security posture, network management, account administration, reliability, collaborative information exchange, policy-based networking and economy.

Security Posture

A superior security posture is attainable with a directory-service architecture utilizing the modular structure of container objects (Organizations and Organizational Units). An organizational unit of the directory can be isolated for administration and access control. These containers as well as other logical objects have access-control permissions, properties, and attributes that permit comprehensive security.

[2] IETF standards - "X.500 Distributed Directory, Directory Access Protocol, and Lightweight Directory Access Protocol"
[3] DMTF specifications - "Directory Enabled Networks, Common Information Model, and Web Based Enterprise Management"

Each directory object has rights and permissions to allow secure use. Directory rights and permissions are similar to file-system permissions in that access-control lists permit user-access and administrative control. Object properties and logical-object associations defined by the directory schema are the basis of policy-based-networking. Policies can be applied to dynamically permit or restrict access, function or view of logical-objects.

Network Management

Superior network management is attainable through a common information model. The common information model permits well-known logical representation of all network elements. The interaction of the information model with policies that pertain to access and configuration of network device parameters permit embedded intelligence.

Account Administration

Directory services provide for delegation of authority based on roles and responsibilities. For example Corporate Process Requirements can be used to model accessibility. Access can be developed based on Non-Sandian, Limited-Access, General-Access, Foreign National, Resident Alien, On-Site Contractor, Visitor or other status. Business rules can be applied through policies to allow access based on global, regional, site or application dependent criteria. This granular control is realized through an extensible schema in which object class, properties and attributes can be defined.

Reliability and Availability

Increased network resource availability can be realized through policy-based networking and directory-enabled applications. The level of recoverability due to the loss of a server or data store hosting an application can be simply illustrated. For example, a logically represented application object associated with specific users or machines could be configured with one or more application sources. When the master source of the application fails or is no longer available, the secondary source continues to provide service. This scenario also serves as an example for load balancing of a provided service for better access and performance. Directory services offer a comprehensive means to achieve network service goals such as 24 X 7 network availability and 99.95% reliability.

Collaborative Information Exchange

Secure collaborative information exchange is possible due to the modular structure of the directory tree. Autonomous areas of administration can be securely maintained while allowing for information exchange with trusted partners. The directory schema and security architecture allow for granular control of whom has access to network resources. Each autonomous area of administration can utilize a unique set of business rules internally and allow controlled access to external associates.

Policy-Based Networking

The structure for policy-based networking is based on logical-object associations in conjunction with conditional parameters. Policies can be global, regional or local and apply to user accounts, machines or services for access and configuration control. Policy-based networking allows integrated Quality of Service (QoS), service provision and configuration of network elements.

Economy

Cost of Ownership is reduced through a single point of administration and the consolidation of disparate directories. Standards-based directories are scalable to global networks providing for distributed administration and centralized management. Distributed administration is attained through directory rights and permissions that define administrative control to an area of the directory and its contents. Centralized management is attained through a common information model and schema that scale to a global enterprise.

Leveraging Directory Service Technologies

Historically network services have been provided for disparate systems with a variety of flat-file directories or data stores. They include network/computer account directories such as the Microsoft NT Security-Account-Manager, the Novell NetWare 3.X Bindery, as well as application-specific databases. Flat-file databases lack a hierarchical distributed architecture. The scope of flat-file directories is confined to limited deployment due to this lack of scalability. In many instances, hundreds of flat-file directories are maintained in a large environment. This matrix of databases necessitates duplication of data and administrative effort. Each data repository must maintain its own copy of common data or require data import and export to distribute common information. In a large network-computing environment, directory services serve to combine multiple flat-file databases into a distributed architecture.

The Internet Engineering Task Force standards[4] and the Distributed Management Task Force specifications[5] provide the framework to build integrated directory-service solutions scalable to global networks. Large network environments may span geographic, political, organizational and functional boundaries. Global or multi-organizational network-computing environments are heterogeneous in nature, and therefore a standards-based approach must be adopted to foster information exchange.

Directory-service solutions offer a hierarchical, object-oriented extensible data-store. A standards-based directory-service architecture would incorporate scalable single sign-on, centralized or decentralized administration and security based on business, organizational or operational structure. The industry Distributed Management Task Force, formally the Desktop Management Task Force, has developed the Directory-Enabled Networks specification as an extension of the Common Information Model specification. The Directory-Enabled Networks specification permits an embedded-intelligence network-management strategy to manage all network elements through policy-based networking.

[4] X.500 Distributed Directory, Directory Access Protocol, and Lightweight Directory Access Protocol
[5] Directory Enabled Networks, Common Information Model, and Web Based Enterprise Management

The most significant advantage of implementing a well-planned directory-service architecture is the functional surety gained by the association or relationships of logically represented objects that enable:

- Superior network resource accessibility
- Superior security model
- Policy-based-networking (Directory-enabled Quality of Service and Service Provisioning)
- Automated desktop and application configuration based on machine ID, login ID or location
- Automated network device configuration based on conditional parameters

These benefits allow for an integrated management methodology that results in more efficient use of network resources.

A network-computing architecture should optimize the production of the business environment that it supports. This is accomplished through network and computing services that allow information to be shared. Directory-service technologies permit the operational models, business rules and geographic constructs of any organization to be molded into the network-computing architecture. Business rules can be applied through the logical structure of the directory information tree. Access control and process flows are enforced by policies applied through logical-object associations.

Directory-service products such as Novell Directory Service eDirectory, Microsoft Active Directory and Sun/Netscape Alliance iPlanet Directory Server confirm the industry adoption of directory-service technologies as a strategic direction in network design. The investment in directory-service technologies of the leading industry players foreshadows the shift from device-centric network management to a logical management model that represents the entire network. A directory-service requires an information model to define network elements as logical objects. Industry standardization and vendor adoption of directory-service technologies sets the stage for management of all network elements beneath a directory-service architecture.

The magnitude of a unified directory-service architecture that incorporates multiple disparate organizations dictates that standards-based heterogeneity and directory interoperation are fundamental to the directory design. This approach is an integral piece to a directory-service strategy where interoperation and collaborative computing between disparate business functions is a factor. From a Sandia IIS perspective, this would permit increased network-computing service to the scientific community.

Directory services are at the core of current Sun/Netscape Alliance, Microsoft and Novell network-operating environments. These directory services products support LDAP version 3. LDAP version 3 provides X.500 directory query and response access, but this offers limited interoperability. Unfortunately not all directory-service vendors adhere to recommended directory-service standards. This poses problems regarding network services for large heterogeneous environments. To overcome these hurdles, emphasis must be placed on planning for interoperability with techniques such as common naming, equivalence in directory-tree structure, and standards-based design.

An understanding of the corporate business operation models and rules must be incorporated into a directory-tree structure. The interdependencies of various business operations will be used as the framework to define accessibility guidelines for the enterprise.

An enterprise directory-service solution has tremendous merit but poses comparable risk and complexity. Comprehensive planning with thorough design and evaluation of proposed security, accessibility and migration methods are essential to the successful rollout of an enterprise or global directory-service project. The complexity and scope of an enterprise directory-service solution must not be underestimated. Inter-departmental corporate support for such an undertaking is essential to the success of a complete, integrated directory-service design.

The Microsoft NT architecture is one of the cornerstones of Sandia's corporate computing environment, and therefore Microsoft Windows 2000 is an undeniable element in the network-computing equation. The risk in basing an enterprise or unified directory-service solution on Microsoft Active Directory is that Active Directory is Microsoft centric. Microsoft Active Directory only supports Windows 2000 with full directory functionality. Microsoft NT is supported in mixed mode with legacy authentication and Microsoft NT Primary Domain Controller emulation.

When faced with a heterogeneous environment, all computing platforms and business models must be considered. The broad scope of a unified directory solution incorporating the DOE NWC must address existing computing platforms. The primary goal of a unified directory solution is to gel authentication, security, access, and usability for disparate computing platforms with a cohesive manageable schema. A heterogeneous unified directory-service solution could take many forms depending on the technical architecture investment of various organizations or areas of administrative jurisdiction. The objective is to have an integrated information strategy inherent to the directory-service design for a large computing environment.

The following discussion briefly represents possible directory-service scenarios.

Multiple Integrated Directories

- Microsoft Active Directory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Sun/Netscape Alliance iPlanet Directory Server as the primary directory for the UNIX and Linux environments.
- Novell Directory Services eDirectory as the primary directory in areas of jurisdiction invested in a heterogeneous environment.

Dual Integrated Directories

- Microsoft Active Directory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Novell Directory Services eDirectory as the primary directory for the UNIX and Linux environments and in areas of jurisdiction heavily invested in a heterogeneous environment.

Or

- Microsoft Active Directory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Sun/Netscape Alliance iPlanet Directory Server as the primary directory for the UNIX and Linux environments and in areas of jurisdiction heavily invested in a heterogeneous environment.

Or

- Novell Directory Services eDirectory as the primary directory in areas of jurisdiction invested in Windows 2000.
- Sun/Netscape Alliance iPlanet Directory Server as the primary directory for the UNIX and Linux environments and in areas of jurisdiction heavily invested in a heterogeneous environment.

Single Integrated Directory—Novell Directory Services eDirectory

- Novell Directory Services eDirectory is unique among directory-service products in that it is designed to support heterogeneity and a full-featured set of services. LDAPv3 is supported as a core Novell Directory Services eDirectory protocol. Novell Directory Services eDirectory can be hosted on the following computing platforms independent of Novell NetWare 5.X.
  - Microsoft Windows NT
  - Microsoft Windows 2000
  - Sun Solaris
  - Red Hat Linux

To address the scope and complexity of a heterogeneous directory-service environment that encompasses disparate operations and organizations, a complete inventory of business, operational, computing and inter-relational dependencies must be outlined. The directory-tree structure with logical objects representing all network elements, including people, should be modeled to ensure efficiency of design for usability, accessibility, security and administration.

Directory-service technologies leverage the aggregation of logical-object associations to effectively manage global network computing. A logically represented network-computing environment permits identity and profile management, network resource policy management and dynamic service provision. A directory-enabled networking design philosophy provides a distributed administration yet centrally managed architecture.

When considering a corporate, enterprise or global directory solution, all available solutions must be evaluated. The need for this is multi-fold:

- To ensure that a standards-based, vendor-independent solution is pursued.
- To address business, scientific, programmatic and operational computing concerns.
- To ensure that directory-service technologies are leveraged to the best possible advantage.
- To ensure the cohesive application of security and administrative models across all administrative areas.
- To ensure that a knowledgeable, practical directory-solution decision is reached to protect the interests and investments of the various administrative jurisdiction areas (e.g. DOE, SNL/NM, SNL/CA, LANL & LLNL)
- To minimize complexity and implementation with an integrated project approach.

Directory-service technologies are challenging and the learning curve can be intimidating. Implementation requires significant planning and preparation involving business operation models and an understanding of interdependencies. For Sandia this represents a significant transition enforcing an enterprise design philosophy.

Sandia's Existing Microsoft NT Domain Structure

A simple illustration of Sandia's Microsoft NT domain architecture is presented indicating the flat-file architecture. A flat-file architecture is analogous to a flat network. The scalability of the flat-file architecture is limited when compared to the scalability of a hierarchical distributed directory service.

Sandia Microsoft NT Domain Architecture

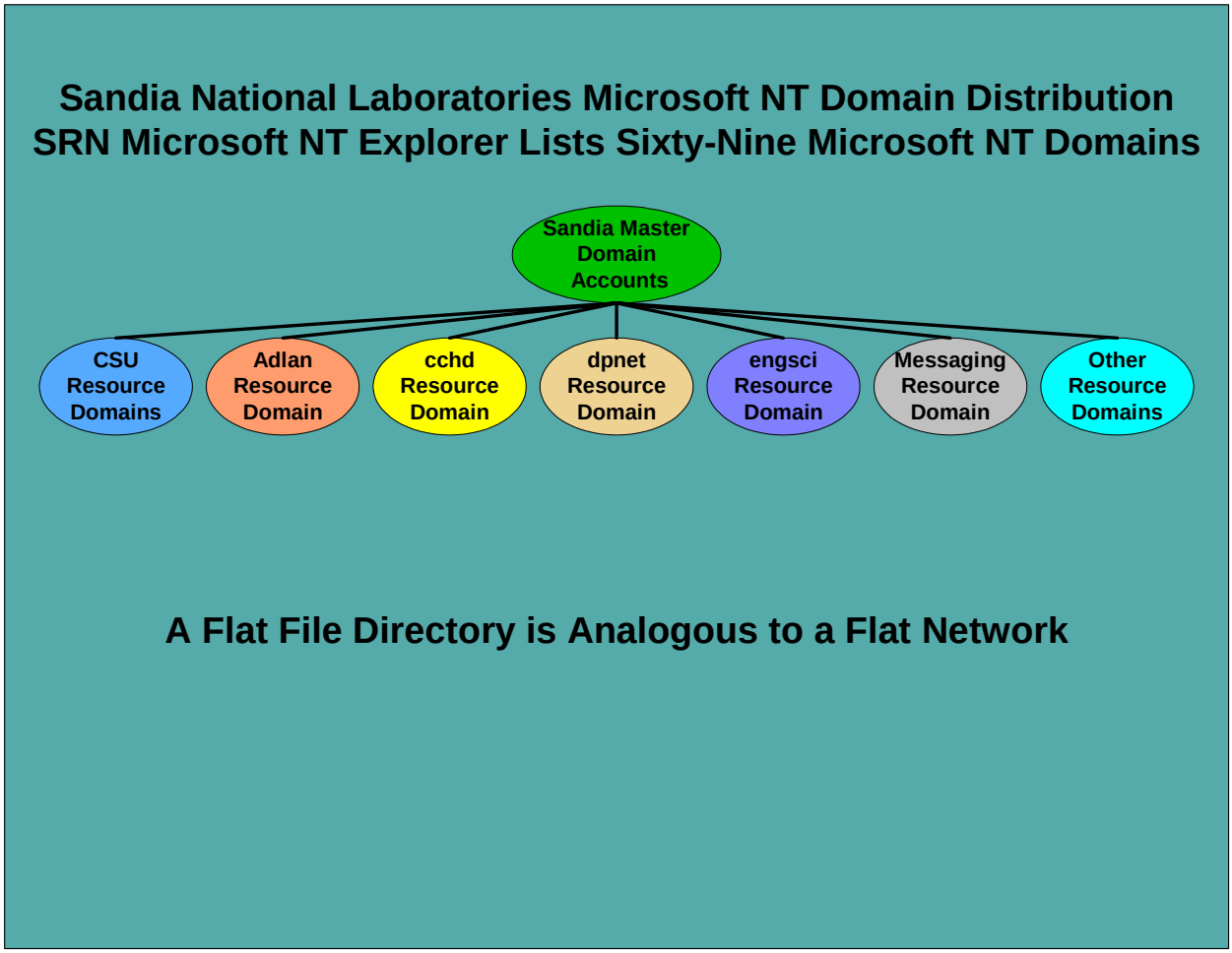

Figure 17

Directory Service Design Requirements

The following is the set of design requirements for an enterprise or multi-organizational directory service. These requirements are based on an industry standards design approach as the foundation for a distributed enterprise network-computing environment.

A directory-service design shall adhere to industry standards and common-information model criteria to foster integration of the full network-computing environment. This will ensure interoperability and minimize sole source dependence. Interoperation of multiple directory services is required for an encompassing heterogeneous network environment.

Impact to the existing network architecture when introducing new technologies shall be evaluated prior to implementation. This will limit the exposure to compatibility and interoperation problems.

Directory-enabled networking design efforts entail a five-year life cycle. Short sited planning will result in the loss of potential benefit of a fully integrated network environment.

All network-computing communities shall be represented in a directory-service design. Buy in by key departments such as human resources is essential to resolve issues such as data ownership. Individual areas of jurisdiction require representation to design an inclusive multiple-organization directory-service strategy.

All incumbent network-computing platforms shall be represented and considered in a directory-service design. A complete directory-service solution will encompasses all computing platforms and includes Sandia California and remote sites. An enterprise directory-service strategy must address the heterogeneity of an enterprise or multi-organization network-computing environment that encompasses multiple computing and network platforms.

Network design goals and objectives shall be defined, including network reliability (e.g., 99.95%) and availability (e.g., 7X24) goals as well as network service strategic direction.

User stratification and administration issues shall be audited to determine enterprise and multiple organization directory-accessibility requirements. An understanding of departmental responsibilities and business process interdependencies will be the basis to design a directory access and security strategy. Organizational function and operation interdependencies must be audited, documented and incorporated into a directory-service design strategy.

Network and computer security issues shall be audited to determine security requirements. A comprehensive security-plan will outline enterprise-layered security. A layered security plan will consider the OSI network model layers; Application; Presentation; Session; Transport; Network; Datalink & Physical and the ARPA TCP/IP model layers; Application Services; Host to Host; Internetwork and Network Access for network security integration.

Application and service distribution for departmental, programmatic and organizational functional levels shall be mapped to determine directory-enabled applications and policy-based-networking strategies. This requires identification of mission critical applications, definition of

network traffic characteristics and prioritization of network services with regard to network service clients.

Security Considerations

Directory services can significantly enhance network and computer security. Careful planning in systems engineering will result in a secured, controlled and useable network-computing environment.

Directory services and directory-enabled networks allow for a high degree of flexibility in security administration. The logical security model overlies the network-operating system, file-system and physical security. This has the effect of fortifying computer and network security with a layer of distributed security that can be applied at a granular level through access control lists and conditional parameters.

Security administration models and administrative jurisdiction need to be well defined to ensure integrity and confidence in the overall security plan. A well-planned administration policy and policy to authority map are key to resolving and documenting these issues.

Security will need to be scrutinized for layered efficiency. For example access-control lists may need to be modified to ensure proper filtering and permission of TCP/UDP port 53 domain packets or the Service Advertisement Protocol. A well-prepared security plan will ensure a controlled security posture and disparate security model interoperation.

A security plan outlining how the various security layers integrate for a strong security posture will be required as illustrated in Figure 18. The security plan should consider the following:

- Directory-service security
- Distributed-Computing Environment security
- Application security
- Network security
- Network-operating-system security
- Operating-system security
- Distributed-file-system security
- File-system security
- Computer security
- Physical security

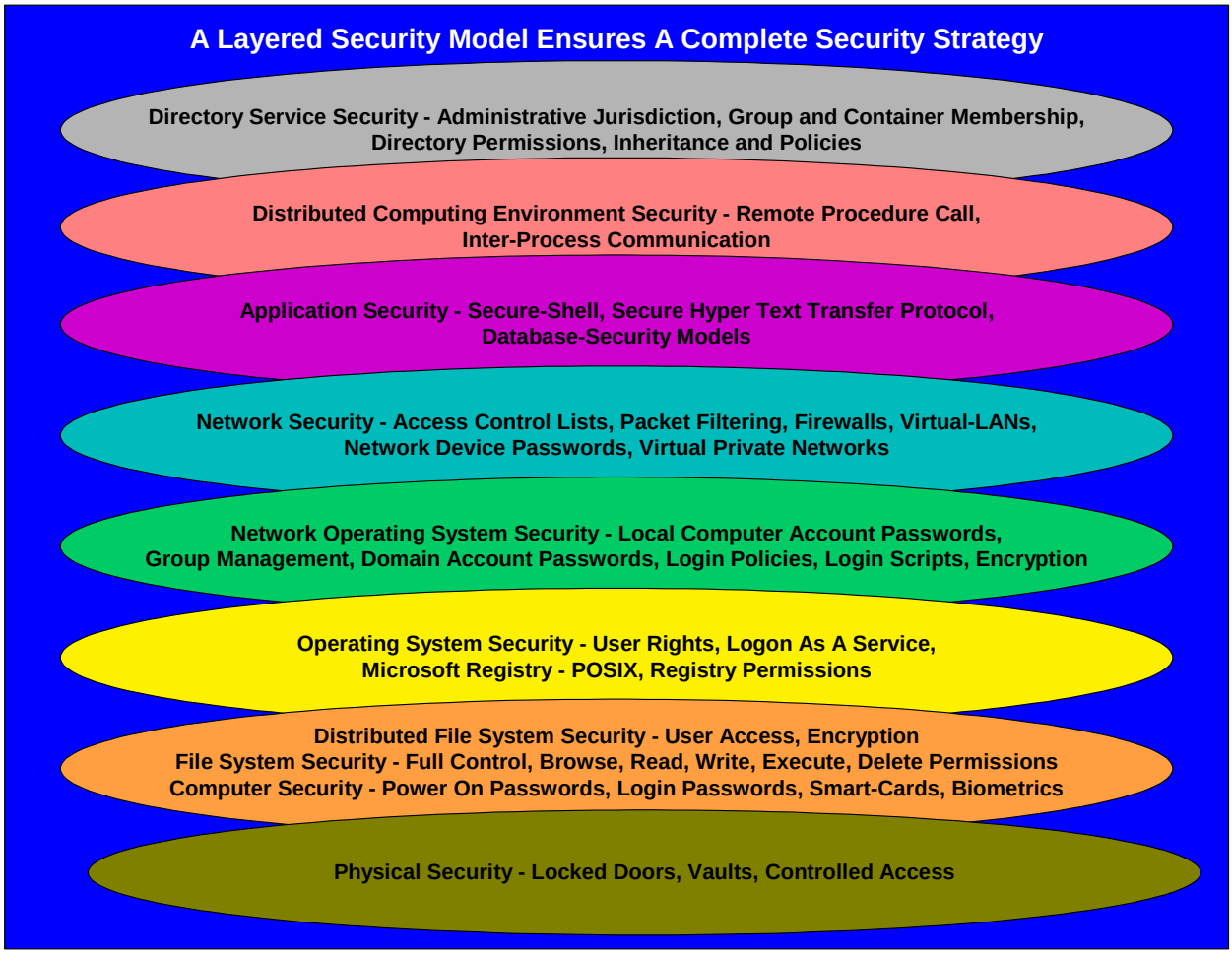

Figure 18

Sandia's Microsoft Active Directory Service-Design Issues

The Microsoft Active Directory tree structure is based on the Domain Name System (DNS) domain structure. This complicates implementation due to DNS design issues in Sandia's multi-site heterogeneous environment.

Active Directory Domain tree pruning and grafting are not available at this time. This poses problems with incorporating existing domains into an Active Directory tree and limits scalability.

DNS integration into Active Directory limits Berkeley Internet Name Domain (BIND) compatibility. This is an issue because Sandia's DNS servers are UNIX/BIND based.

The Sandia NetWork Information System auto updates the DNS with NetWork Information System registered host names. This introduces complications with Microsoft Active Directory interaction with dynamic DNS updates.

Microsoft Active Directory is Windows 2000 centric. A supplemental directory-service architecture would be required to support UNIX, Linux, Apple and the scientific computing communities.

The Sandia National Laboratories Internet and Intranet DNS structure will be heavily impacted by the implementation of Microsoft Active Directory Services.

Existing DNS issues complicate design efforts; these issues include the following. Host names can be duplicated, one at the SNL/NM site and another at the SNL/CA site. Depending on the DNS server that responds to the resolver first, the name query may be resolved to the wrong host (e.g. a SNL/NM host trying to reach a SNL/CA host). Duplicate host names registered to Sandia may have an impact to licensing compliance.

Numerous Microsoft NT domains complicate the migration of the Sandia Microsoft NT computing environment to Microsoft Windows 2000 and Active Directory. There are sixty-nine Microsoft Windows NT domains in the Sandia Restricted Network environment. This presents a significant migration burden to transition to a complete Windows 2000 model in which Active Directory can be fully exploited.

Microsoft Active Directory and DNS integration/management should be considered for performance and overhead in a large environment. Active Directory relies heavily on DNS, therefore performance issues and impact to the full network-computing environment should be evaluated.

Significant training and planning is required for a Microsoft Active Directory design and implementation project.

Microsoft Active Directory is a new technology and is not yet implemented in the Sandia corporate computing environment.

It is important to note that Windows 2000 can be deployed while supporting the current Microsoft Windows NT domain structure. This means that Windows 2000 deployment can proceed separately from a Microsoft Active Directory deployment.

Sandia's Novell Directory-Service Design Issues

Novell Directory Services are no longer implemented in the Sandia corporate computing environment.

Cross platform Novell Directory Services (NDS) support requires significant expertise.

Novell Single-Sign On (SSO) would require operating system and application integration planning.

Novell NDS for NT running in a Windows 2000 environment poses an unknown incompatibility risk.

Significant training and planning is required for a Novell Directory Services eDirectory design and implementation project.

Directory-Enabled Application Issues

Sandia is facing directory-enabled application issues as legacy applications age out and directory-enabled application platforms become available. This is the case with NetDynamics, which is being replaced with the Sun/Netscape Alliance iPlanet Application server.

IBM WebSphere and BEA Systems Weblogic Server are other middleware products that are directory enabled. IBM WebSphere is provided with Novell eDirectory Services. Directory services are an integral component of integrated management for a web-enabled enterprise infrastructure as applied to both integrated client/server applications and Internet-based approaches such as Intranets and extranets.

Directory-Service Implementation Issues

The adoption of an enterprise network design ideology requires acceptance from the Chief Information Office and supporting organizations.

Barriers with inter-departmental communication need to be resolved to settle issues of data ownership.

DOE NWC Directory-Service Architecture

Sandia is at a crucial juncture and presented with the opportunity to pilot an evaluation and design of a DOE NWC collaborative directory-based network. A directory-service architecture could significantly improve collaborative computing with regards to ASCI and DISCOM activities. Such a directory structure could be of benefit for inter-site authentication. The collective involvement of each organization is the basis for a complete design. Disparate security models and business rules need to be scrutinized and incorporated into the directory structure to ensure security and function. A standards-based ideology would promote collaborative information exchange and ensure interoperation with external network environments. A unified directory-service design must consider the heterogeneous nature of a multiple-organization-computing environment and thus must seek to integrate information.

Directory interoperation can be achieved through two systems engineering approaches:

- The use of metadirectory tools as a clearinghouse for multiple directories
- A directory interoperation design approach that incorporates industry standards, common naming and equivalence in directory tree design

An integrated directory-service design strategy is essential to a collaborative enterprise or global network computing architecture.

DOE NWC Unified Directory-Service Design Issues

Enfranchising a multi-organizational network design is difficult and requires significant collaboration. Coordination and project focus may be difficult to maintain across operational boundaries.

Significant training and planning is required for a unified directory-service design and implementation project.

Directory-Service Project Challenges

The design of a global or multi-organizational directory-service solution is a major undertaking. Extensive planning, evaluation, and training are needed to produce a viable enterprise directory-service design. The complexity of a directory-service design project for a multiple organization network requires purposeful systems engineering to address the needs of the full environment. Collaboration of key network-computing interests requires significant commitment. Commitment from each organization within the company is required to successfully implement an enterprise directory architecture. A unified directory-service architecture encompassing the DOE NWC will require a concerted effort involving representation of all network-computing interests.

The complexity and scope of implementing an enterprise directory-service solution is substantial. The magnitude of incorporating a directory-service architecture is equivalent to a redesign of network services. The paradigm of a directory service architecture design involves incorporating business processes and workflow into the delivery of network-computing services. The risk lies in underestimating the complexity, coordination and commitment required for successful implementation. The technical challenges are outweighed by the organizational challenges in soliciting support and commitment.

Network service design changes including the DNS and Dynamic Host Configuration Protocol will have significant impact to the standing technology architecture. Design changes should be considered carefully and with discretion given to an overall network service plan.

The learning curve to understand directory services over an already complex technical environment is substantial. Training is essential to bring technical staff up to speed.

Incorporating a full network approach is difficult and requires significant collaboration and research to audit existing network-computing architectures and business processes. The current state of the network must be understood to develop a directory-service migration plan.

Resources needed to evaluate, plan and implement such encompassing technology are significant.

In-house applications that need to be directory enabled would present a training and conversion burden.

Directory-account and access-management options must be scrutinized for compatibility and conflicts with the Distributed Computing Environment and the Entrust X.500 Directory environment.

Recommendations

Based on the industry adoption of directory-service technologies it is recommended that:

Sandia adopt a directory-enabled networking design philosophy to invest in policy-based-networking, quality of service, strengthened security posture and comprehensive network management. This will entail a technology investigation into Cisco Networking Services, Cisco Architecture for Voice, Video and Integrated Data and Cisco Quality Policy Manager.

Directory-service products should be evaluated to determine best fit and function to address the full network-computing environment. The product evaluation will yield conclusions, recommendations, risks and benefits of various directory-service implementation models.

Sandia adopt a formal application review process. This would involve application profiles to determine the impact to network services and to ensure that an application is optimized for network integration.

Sandia adopt a formal schema review process to ensure that the schema design is optimized for the directory enabled network environment.

Sandia pursue the implementation of directory-enabled applications. Workflow and web-based applications can be assessed for directory service integration.

A standards-based Department of Energy Tri-labs directory-service solution should be considered to achieve a collaborative network-computing environment.

A purposeful system engineering approach should be applied to the introduction of directory-service technologies due to the complexity and far-reaching impact on all aspects of the network-computing environment.

An evaluation plan defining objectives, resources, schedule and project scope should be written to address project-planning and system-engineering processes. Metrics for comparison of each of the implementation models should be written to facilitate design review and selection.

A project team representative of appropriate technical and operations personnel should be assembled to address enterprise and integrated directory-service design strategies.

Third party solutions such as Oblix, Inc (http://www.oblix.com) Oblix Service Center and Oblix Publisher, and Access360 (http://www.access360.com) enRole bridging software should be evaluated to determine the best course of action to integrate directory information.

A comprehensive security plan should be developed to outline how various security models layer and integrate for a strong security posture.

Summary

Reliance on information systems has become critical for day-to-day business operations and scientific computing. Directory services offer enhanced reliability and availability through logical representation of network elements. A standards-based directory-service design approach will ensure directory interoperation and sound directory design. Directory services provide the technologies for comprehensive network management, single sign-on, superior security posture, and integrated user administration that facilitate reduction in total cost of ownership.

The industry is building around these initiatives and the investment of the leading network-operating system vendor's flag the transition from device-centric network management to a "manage-the-network" philosophy. Directory-service technologies are impacting network management and service delivery through the DMTF Directory-Enabled Networks specification. Directory-service technologies are impacting e-commerce, multi-platform collaborative computing, and network account administration through products such as Sun/Netscape iPlanet Directory Server, Microsoft Active Directory and Novell eDirectory Services.

Sandia must consider the importance of directory-service technologies and respond appropriately. The time to act is now, while Sandia is ahead of the curve in implementing directory-service technologies. Managing information in today's connected world is vital to Sandia's mission to provide exceptional service in the national interest.

The Department of Energy and scientific partners can leverage the hierarchical structure of directory services to attain superior security and enhance collaborative information exchange. The flexibility of distributed administration and centralized management allows for reliable, secure user stratification. Commercial companies as well as government agencies including the Department of Defense are actively pursuing directory-service infrastructures for collaborative information exchange.

Conclusions

The industry's leading network and computing vendors are developing products to take advantage of directory-service technologies. Sandia must begin planning to incorporate directory-service technologies in the corporate and scientific computing environments.

The benefits to be gained are significant with directory-service technologies, but the risk is proportionate to the gain. Care must taken in the planning and implementation of such encompassing technologies. A hurried approach is fraught with risk, therefore a well-prepared strategy is imperative.

The complete environment must be considered with the introduction of directory-service technologies into an enterprise heterogeneous network-computing environment. An understanding of the full complement of customers, systems, applications, security and network services is the baseline for directory-services policy-based networking planning, design and implementation.

Technical References

Sandia National Laboratories Technical Reference Documents:

Sandia Server Consistency Team Standard Server Naming Convention, October 1998

Sandia National Laboratories Network Naming Conventions Procedure & Policy,
M. J. Ernest, February 2, 1990

Sandia Materials And Process Sciences Network Integrated Microsoft NT, UNIX and Apple TCP/IP Novell NDS design, Curtis Keliiaa, Ed Klaus, Tim MacAlpine
September 7, 1996

Sandia Common Naming Convention report,
Curtis Keliiaa, Larry Tolendino, September, 1997

Sandia Telecommunication Operations ISO 9000 Network Design Change Management Process, Bruce C. Whittet, Process Owner, June 5, 2000

Sandia Telecommunication Operations ISO 9000 Design/Evaluation/Development Process, Pat Manke - Process Owner, May 19, 2000

Published Material:

Understanding Directory Services
By New Riders Publishing
Copyright © 2000

DNS and BIND
O'Reilly & associates, Inc
Copyright © 1992

Directory Enabled Networks, John Strassner, Cisco Systems
Macmillan Technical Publishing
Copyright © 1999
ISBN 1-57870-140-6

Windows 2000 Active Directory
O'Reilly & associates, Inc
Copyright © 2000
ISBN 1-56592-638-2

Cisco Internetworking with Windows NT & 2000
The McGraw-Hill Companies
Copyright © 2000

Industry Task Force, Working Groups, Standards and Specifications

- Directory Enabled Networks Ad Hoc Working group Web Page:
  - http://murchiso.com/den/
- Distributed Management Task Force, Inc. DMTF Web Page
  - http://www.dmtf.org/
- DMTF DEN Web Page:
  - http://www.dmtf.org/spec/denh.html
- DMTF CIM Standards Web Page:
  - http://www.dmtf.org/spec/cims.html
- DMTF WBEM Standards Web Page:
  - http://www.dmtf.org/spec/wbem.html
- Internet Engineering Task Force Web Page
  - http://www.ietf.org/
- Internet Architecture Board Web Page:
  - http://www.iab.org/iab/
- Internet assigned Numbers Authority Web Page:
  - http://www.iana.org/

X.500 Specification

- International Telecommunications Union:
  - http://www.itu.int/
- International Telecommunications Union "Series X Recommendations: X.500 and up"
  - http://www.itu.int/plweb-cgi/fastweb?getdoc+view1+itudoc+27972+0++X.500
- International Organization for Standardization (ISO)
  - http://www.iso.ch/
- NEXOR Industry Information " X.500 and Internet Directories"
  - http://www.nexor.com/index1.htm

Directory Service Vendors

- Microsoft Web Page:
  - http://www.microsoft.com/
- Microsoft Windows 2000 Web Page:
  - http://www.microsoft.com/windows2000/library/planning/default.asp
- Sun/Netscape Alliance Directory and LDAP Web Page:
  - http://developer.netscape.com/tech/directory/index.html?cp=dev01mtec
- Novell Web Page:
  - http://www.novell.com/
- NDS eDirectory™ Design 2000 Web Page:
  - http://www.novell.com/products/nds/nds-design-2000.html

Industry Reviews

- Network Magazine "2000 Products of the Year awards"
  - http://www.networkmagazine.com/magazine/current/0005year.htm
- Network Computing Magazine OSes & Network Services Web Page:
  - http://www.networkcomputing.com/core/core1.html
- Network Computing Magazine " Redefining the NOS"
  - http://www.nwc.com/1110/1110f1.html
- Network Computing Magazine "May 15, 2000 Well-Connected Awards"
  - http://www.nwc.com/1109/1109well-conn.html
- Network Computing Magazine "Windows 2000: Worth the Pain (Almost)"
  - http://www.networkcomputing.com/1104/1104f1.html
- Network Computing Magazine "Directory Services: The Active Directory"
  - http://www.networkcomputing.com/netdesign/1013nt5.html
- Network Computing Magazine "The Cross-Platform Challenge"
  - http://www.networkcomputing.com/1116/1116f2.html
- NetWorldFusion "LDAP Untangled"
  - http://www.nwfusion.com/reviews/2000/0515rev1.html

Related Information

- InternetWeek " Technology Is Just One Obstacle For Enterprise Directories"
  - http://www.techweb.com/wire/story/TWB20000725S0003
- InternetWeek " Directories Stand Guard -- Software primed for intercompany e-business"
  - http://www.techweb.com/se/directlink.cgi?INW20000724S0001
- Federal Computer Week "Building an agency metadirectory - Defense Information Systems Agency tackles enterprise wide network directory"
  - http://www.fcw.com/fcw/articles/2000/0501/tec-meta-05-01-00.asp
- Globus Directory Enabled Research & Development Environment
  - http://www.globus.org/
- Network Computing Magazine "Management Standards Come Together"
  - http://www.networkcomputing.com/1117/1117f3.html

RFC References

- The IETF Request For Comments Web Page:
  - http://www.ietf.org/rfc.html
- LDAP Documentation and Related RFC's:
  - http://www.umich.edu/~dirsvcs/ldap/doc/index.html
- The IETF Current Internet-Drafts Web Page:
  - http://www.ietf.org/1id-abstracts.html

NOVELL DIRECTORY SERVICE eDIRECTORY AND MICROSOFT ACTIVE DIRECTORY SERVICE PRODUCT FEATURE COMPARISON

The following are a side-by-side feature comparison of Novell Directory Services eDirectory and Microsoft Active Directory Service. This information is provided to show the rich feature set that these products offer. Both Novell and Microsoft develop for Lightweight Directory Access Protocol, Common Information Model and Directory Enabled Networks compatibility. The Strengths and Limitations comparison sections represent the opinions of the author based on product research.

Novell Directory Service eDirectory

Directory Structure

- X.500 style Name Space
- Directory Structure flexible based on:
  - Geographical Layout - Albuquerque, Tech Area 1, CSU880, Carlsbad, Livermore etc.
  - Operational Layout
  - Functional or Work Group
- NDS eDirectory based on the Oracle Database Engine
- NDS eDirectory is independent of NetWare.
- NDS eDirectory can be hosted from Sun Solaris, Linux, Microsoft Windows NT or Windows 2000.
- Circular Containment - Organizational Units (OU) can contain domains and nested OU's.

Microsoft Active Directory Service

Directory Structure

- Active Directory Domain Tree
- Name Space tied to Domain Name Service structure.
- Directory Tree structure tied to DNS domain structure. For Root - Registered DNS domain, Delegated Sub Domain, Reserved Private.
- Directory Tree structure tied to DNS domain structure.
- Accommodate distinct DNS names to use multiple Directory Trees
- ADS based on the Extensible Storage Engine

Novell Directory Service eDirectory

Partition Types

- [ROOT] partition
- Directory partitions - design to limit replication synchronization traffic.

Directory Replica Types

- Master Replica
- Read Write Replica
- Read Only Replica
- Subordinate Reference Replica - For Directory Tree Walking between partitions
- Sparse Replicas - LDUP component, customizable partial replica for directory search and query. Can replace catalogs and be scoped to a particular subset of objects.
- Replica Filters - allows creation of a replica that is both sparse and fractional (specified attributes)

Replication Method

- Master Replica
- Read/Write Replica
- Read Only Replica
- Subordinate Reference Replica - Tree Walking
- Time Stamp Dependant Replication
- WAN Interval settings

Microsoft Active Directory Service

Partition Types

- Schema Partition - Object and attribute definitions
- Config Partition - Active Directory structure, Sites & Domains
- Domain Partition - Domain specific objects such as organizational units (OU), users, groups and computers.
- Domain Components - equivalent to DNS zones (sandia.gov)
- ADS Domain Forest
- ADS Domain Tree
- ADS Domain
- Operations Masters - (Flexible Single Master Operation (FSMO) roles)
- Infrastructure Operations Master - Assigns Security IDs.

Directory Replica Types

- Multi-master Replica's

Replication Method

- Peer to peer multi-master replication
- Transitive Trust Relationships

Novell Directory Service eDirectory

Security

- NDS Permissions
  - Object Rights - Read, Create, Write, Add-self, Supervisor
  - Property Rights - Browse, Compare, Delete, Rename, Supervisor
  - Inheritance
    - NDS - Inheritance Rights Filters
- Administrative Delegation - Groups or users assigned as a trustee of an object.
- Organizational Roles
- Aliasing
- [ROOT] - Supervisor Rights
  - NDS supervisor right transcends to the file system
- Organizational Unit Administrators
- Organizational Unit Forms natural groups

Microsoft Active Directory Service

Security

- ADS Permissions
  - Full Control
  - Read
  - Write
  - Advanced
    - Object Type Extended Permissions
- Defaults for Authenticated Users
  - Read
- Defaults for Administrators
  - Read
  - Write
  - Create ACL
- Defaults for Domain Administrators
  - Full Control
  - Read
  - Write
  - CACL
  - DACL
- Defaults for Enterprise Administrators (Inherited)
  - Full Control
  - Read
  - Write
  - CACL
  - DACL
- Security Descriptor
  - Defines Access & Permissions
  - Security ID's
  - Relative ID's
- Security Principles
  - Users
  - Groups
  - Computers
- Inheritance
  - Inheritance Blocking
- Inheritance Override Discretionary ACL
  - Applies to Objects, Attributes & Object Classes
- System ACL
  - Event Auditing

Novell Directory Service eDirectory

Encryption

- Novell International Cryptographic Infrastructure - plugs into NetWare Modular Security Service to provide 56 bit to unlimited strength with:
  - DES
  - 3DES
  - RC2/RC4
- RSA
- MD5
- Secure Sockets Layer (SSL) 3.0
- LDAP over SSL
- Public Key Cryptography Standards (PKCS)

Logical Objects

- World ([ROOT]
- Country
- Locality
- Organization
- Organizational Units - Natural group, all members in a domain have permission to resources in that domain.
- Leaf Objects
  - Users
  - Groups
  - Computers
  - Servers
  - Organizational Roles
  - Alias'
  - Volumes
  - Profiles
  - Printers
  - Print Server
  - Print Queue
  - Directory Map
  - Applications

Microsoft Active Directory Service

Encryption

- RSA
- MD5
- Secure Sockets Layer (SSL) 3.0

Logical Objects

- Active Directory Domains
- Organizational Units
- Leaf Objects
  - Users
  - Groups
  - Computers
  - Servers
  - Group Policies
- Group Types
  - Universal Groups
  - Global Group
  - Domain Local group
  - Nested Groups

Novell Directory Service eDirectory

Authentication

- Public Key Infrastructure Services X.509 V3
  - Certificate Authority
- Smartcards
- Kerberos
- User Authentication Module (UAM)/Redirection
- NetWare Modular Authentication Service (NMAS)
  - Password
  - Biometric Token
  - Clearance Level
  - Logged In
  - Matched to NDS Partition and Volume Grade for permissions:
    - NoAccess
    - Read/Write
    - Read
  - Graded Authentication
    - Grades
    - Security Levels
    - Clearance Levels
    - Authentication Policies
  - Login Method Container Object
  - Login Policy Object - Login Sequence
  - Apply Graded Authentication Labels to Volume Objects, Partitions and User Objects
- Solaris and Linux
  - Pluggable Authentication Modules (PAM)

Microsoft Active Directory Service

Authentication

- Public Key Infrastructure Services X.509 V3
  - Certificate Authority
- Kerberos
- NTLM
- Smartcards

Novell Directory Service eDirectory

Directory Support Services

- DS Expert: NetPro's NDS Proactive Monitoring Tool
- DS Browse Tool
- DS View
- DS Dump
- DSREPAIR NLM
- Internationalization - Supports Four Languages
- LDAP Version 3.0 supported as a core protocol.
- DirXML - enables multiple NDS tree or other directory data synchronization.
- NDS Federation - allows access to another NDS tree without using data synchronization.
- WebDAV - Web based Distributed authoring and Versioning
- Novell Single-Sign On (SSO) - Maintains a 3DES secret-data store to automatically retrieve frequently used passwords

Microsoft Active Directory Service

Directory Support Services

- DS Repair Mode - F8
- Replication Method
  - Multi-Master Replication
    - Schema Partition
    - Configuration Partition
    - Domain Partition
    - Partial Domain Directory Partition (Global Catalog)
- Group Policies - Group Policy Object - Published & Assigned
  - Logon/Logoff scripts
  - Registry dependent
  - Local System Policies
- IP/RPC (DS-RPC) or Inter-site Mechanism (ISM) SMTP Transports for WAN link replication.
- Knowledge Consistency Checker (KCC) - Auto Generation of replication topology, manages connections - links connecting replication partners.
- Directory synchronization - Inter directory information
- LDAP Version 3.0 Compliant
- WebDAV - Web based Distributed authoring and Versioning

Novell Directory Service eDirectory

System Administration

- NWAdmin management application
- NetWare Management Portal (NMP) - Web based management tool
- Console1 - Web Based Management Console
- Java Based Management Console
- NetWare Console
- NetWare Enterprise Web Server
- Login Scripts
  - Container Login Script
  - Profile Login Script
  - User Login Script

Client Support

- NDS Corporate Edition
  - Microsoft 9x
  - Microsoft NT
  - eDirectory For NT
    - Corporate edition allows domain users and other NT resources into the NDS tree. Allows heterogeneous/NT networks to be centrally managed.
    - NDS for NT replaces the samserv.dll
  - Microsoft 2000
  - Unix
  - Linux
  - IBM's RS/6000 systems
- Apple (3rd Party)

Microsoft Active Directory Service

System Administration

- Microsoft Management Console (MMC)
  - Users & Computers
  - Site & Services
  - Domains & Trusts
  - Group Policy Snap in
- Enterprise Admins
- Domain Admins
- Schema Admins
- Administrative Delegation
  - Delegation Control Wizard
  - Centralized Administration
  - Decentralized Administration
- Login Scripts
  - MMC - Windows Settings Logon & Logoff Scripts
  - Specified to run synchronously or asynchronously in the User Configuration Administrative Templates section of the Group Policy Object.

Client Support

- Microsoft 2000
- NT Domain Emulation
- Directory-services client to support Browse directory-service, DFS and change passwords on any Domain Controller.

Novell Directory Service eDirectory

Catalog Services

- Limited Global Catalog Services in NetWare 5 and earlier releases. Novell eDirectory enhances Global Catalog services and adds support for sparse replicas.

Directory Applications

- ZENWorks (Zero Effort Networks)
  - Automated application recovery, installation based on Policy and NT registry settings
  - Fault Tolerant application source
  - Application Object
  - Computer Object
  - Group Object
  - User Object
  - Policy Object
- ZEN for Servers
- ZEN for Networks
- Directory Integrated GroupWise
  - Internet Messaging
    - POP
    - IMAP
- Novell eGuide - LDAP white pages application.
- Novell Digitalme - Directory enabled internet identity management.

Network Services

- DNS/DHCP Services
- Native IP
- Directory Integrated Border Manager
  - Internet Caching
- NetWare Access Policies (3COM partner)
- ZENWorks for Networks
  - Manage Network traffic
  - Store QoS Policies
- XML/DirXML

Microsoft Active Directory Service

Catalog Services

Comprehensive Global Catalog

Directory Applications

- Active Directory Installation Wizard
- Delegation Control Wizard - (suggest managing by group)
- MS Exchange
  - Exchange & ADS based on the Extensible Storage Engine. Microsoft Exchange 2000 is integrated with ADS.
- Internet Messaging
  - POP
  - IMAP
- Replication Monitor - Update Sequence Number (USN) High water mark (plus time stamp for tie breaker)

Network Services

- DNS/DHCP Services
- XML/DCOM
- DirXML

Novell Directory Service eDirectory

File System Support

- Novell File System
  - Block Sub Allocation
  - Compression
  - Near Line Storage
  - File System Rights:
    - Read
    - Write Erase
    - Modify
    - File Scan
    - Supervisor
  - Inheritance Rights Masks
- NetWare Storage System
  - Organized by:
    - Storage Group
    - Provider
    - Volume
  - Journaling File System
  - Fast Volume Mounting - GB in seconds
  - 10^{16} Volume/File size support
  - Does not support Block Sub Allocation
- Distributed File System (DFS) Support
- Storage Management Services
  - Tape Backup

Microsoft Active Directory Service

File System Support

- NT File System
- Distributed File System (DFS) Support
- Dynamic Volumes
- Encrypted File System (EFS)
- NTFS 5 File Permissions
  - Transverse Folder
  - Execute File
  - List Folder
  - Read Data
  - Read Attributes
  - Create Files
  - Write Data
  - Write Attribute
  - Write Attribute
  - Write Ext. Attribute
  - Delete
  - Delete Sub-Folders & Files
  - Read Permissions
  - Change Permissions
  - Take Ownership

Novell Directory Service eDirectory

Industry Partners

- IBM - Websphere
- Oracle - Oracle 8
  - NDS 8 (NW 5.1)
  - WEBDB Oracle Wed Extensions
- Netscape Web Server
- 3COM

Industry Initiatives

- Directory Enable Networks (DEN)
- Common Information Model (CIM)
  - Automated Device Configuration
- Business to Business
  - E-Directory
- DENIM - Directory Enabled Network Infrastructure Model
- NDS for UNIX Tru64 in development

Microsoft Active Directory Service

Industry Partners

- Cisco
- Numerous application developers

Industry Initiatives

- Directory Enable Networks (DEN) - Partnered with Cisco
- Common Information Model (CIM)
  - Automated Device Configuration

Novell Directory Service eDirectory

Limitations

- Limited Application support
- Significant learning curve
- Requires Enterprise level evaluation, planning and functional commitment.
- Novell technical support expertise for Solaris and Linux is limited
- Solaris and Linux Installation tools are not intuitive
- Cross platform implementation requires significant expertise
- Console 1 administration tool is not stable or fully functional in a cross-platform environment

Microsoft Active Directory Service

Limitations

- Significant learning curve
- Requires Enterprise level evaluation, planning and functional commitment.
- No Native ADS support for Windows 9X or NT.
- Usability
  - No Object Copy
  - No drag & drop moves
  - No Alias Objects
- Organizational units - cannot view active permissions.
- No recovery if all or only Root Domain Controller is lost.
- Microsoft is new to the Directory-services arena therefore is still developing industry partners and directory enabled application ISV's.
- Active Directory Domain tree management and merging is difficult.
- Replication becomes difficult in large network environments.
- Active Directory does not adhere strictly to X.500 specifications.
- Directory Tree structure tied to DNS domain structure - a concern is ADS/DNS management overhead, an Active Directory Domain Controller registers 19 or more service records with DNS.
- No use of Universal groups, nested groups or inter-domain group membership in mixed mode.
- Converting to Windows 2000 native mode is non-reversible - verify there are no more Windows NT servers in the environment.
- ADS is Microsoft centric a lacks heterogeneous client support.
- The DNS implementation of Windows 2000 is a non-standard implementation. An "_msdcs" zone is required for Active Directory function.

Novell Directory Service eDirectory

Strengths

- NDS eDirectory is proven scalable and mature.
- Usability
  - Object Copy
  - Object Templates
  - Drag and Drop moves
  - Object Aliasing
- Total Cost of Ownership reduced due to enterprise management strategy.
- Mature Directory services
- Demonstrated support for 1 billion directory objects.
- Platform independence - NDS eDirectory can be hosted from NetWare, Microsoft NT, Microsoft Windows 2000, Sun Solaris and LINUX.
- NDS eDirectory supports LDAPv3 as a core protocol.
- Viable Cross-platform directory service
- Cross-platform authentication is robust
  - Kerberos
  - Public Key Infrastructure Services X.509 V3
  - Kerberos
  - User Authentication Module (UAM)/Redirection
    - NetWare Modular Authentication Service (NMAS)
  - Solaris and Linux
    - Pluggable Authentication Modules (PAM)
- Permits multi-platform Single-Sign On

Industry Awards

- NDS eDirectory - Network Magazine 2000 Products of the Year Award - Server Software category, Network Magazine May 2000.
- NDS eDirectory - Network Computing Well Connected Awards - Software Product of the Year, Network Computing May 15 2000.

Microsoft Active Directory Service

Strengths

- Total Cost of Ownership reduced due to limited enterprise management strategy.
- The Microsoft Management Console (MMC) presents a consistent management interface.
- Under lying repository based on the proven JET database.
- Support for millions of directory objects.
- Active Directory supports LDAPv3 as a core protocol.
- Simpler replication in small to mid sized networks.
- The Kerberos authentication used in Windows2000/Active Directory is much better than Microsoft NT 4 NTLM authentication.

Appendix A
Definition of Acronyms

3DES - Triple Data Encryption Standard

AAA - Autonomous Administration Area
AAP - Administrative Point ACL - Access Control List
ACA - Access Control Areas
ACE - Access Control Entries
ACIA - Access Control Inner Administrative Area
ACP - Access Control Policies
ACSA - Access Control Specific Area
ACSE - Access Control Services Element
ADS - Active Directory Services
ASN.1 - Abstract Syntax Notation One

BIND - Berkeley Internet Name Domain

C - Country
CASA - Collective Attribute Specific Area
CACL - Create Access Control List permission
CIM - Common Information Model
CMIP - Common Object Information Protocol
CN - Common Name
COM - Common Object Model
COPS - Common Open Policy Service
CORBA - Common Object Request Broker Architecture

DACD - Directory Access Control Domain
DACL - Discretionary Access Control List
DAP - Directory Access Protocol
DC - (Microsoft) Domain Component
DCE - Distributed Computing Environment
DCOM - Distributed Common Object Model
DEN - Directory Enabled Networks
DES - Data Encryption Standard
DFS - Distributed File System
DHCP - Dynamic Host Configuration Protocol
DIB - Directory Information Base
DiffServ - Differentiated Services
DISP - Directory Information Shadowing Protocol
DirXml - Directory eXtensible Markup Language
DNS - Domain Name System
DOP - Directory Operational Binding Management Protocol
DSA - Directory Server Agent
DSA - Directory System Agent
DSP - Directory System Protocol
DUA - Directory User Agent

EFS - Encrypted File System

FSMO - Flexible Single Master Operation
FTP - File Transfer Protocol

HTML - HyperText Markup Language
HTTP - HyperText Transfer Protocol
HTTPS - Secure HyperText Transfer Protocol

IAA - Inner Administrative Area
IAP - Inner Administrative Point
IMAP - Internet Messaging Access Protocol
IPSec - IP Security
ISV - Independent Software Vendor

KCC - (Microsoft) Knowledge Consistency Checker

L - Locality
LAN - Local Area Network
LDAP - Lightweight Directory Access Protocol
LDIF - Lightweight Directory Interchange Format
LDUP - Lightweight Directory Duplication/Replication/Update Protocols

MD5 - Message Digest 5
MIB - Management Information Base
MMC - Microsoft Management Console

Appendix A
Definition of Acronyms

NDS - Novell Directory Services
NetBIOS - Network Basic Input Output System
NMAS - (Novell) NetWare Modular Authentication Service
NOS - Network Operating System
NTFS - (Microsoft) New Technologies File System
NTLM - (MSNT) New Technologies LAN Manager

O - Organization
OU - Organizational Unit

PAM - Pluggable Authentication Modules
PKCS - Public Key Cryptography Standards
PKI - Public Key Infrastructure
POP - Post Office Protocol

QoS - Quality of Service

RC2, RC4, RC5 - Rivest, Shamir, Adleman - RSA Data Security, Inc. encryption algorithms
RFC - Request For Comment
RMON - Remote Monitoring
ROSE - Remote Operation Service Element
RSVP - ReSource reserVation Protocol

SAA - Specific Autonomous Area
SACL - System Access Control List
SAP - Specific Administrative Point
SGML - Standardized Generalized Markup Language
SNMP - Simple Network Management Protocol
SNMPConf - Simple Network Management Protocol Configuration
SQL - Sequential Query Language
SSL - Secure Sockets Layer
SSO - Single Sign On

TCP/IP - Transmission Control Protocol/Internet Protocol

UAM - (Novell) User Authentication Module
UDP/IP - User Datagram Protocol/ Internet Protocol
UNC - (Microsoft) Universal Naming Convention
URL - Uniform Resource Locator, AKA Universal Resource Locator
USN - Update Sequence Number

VMPS - Virtual Membership Policy Service
VPN - Virtual Private Network

WAN - Wide Area Network
WBEM - Web Based Enterprise Management
WebDAV - Web Distributed Authoring and Versioning
WebDB - Oracle Web Extensions

X.500 - The Directory: Concepts Models and Services
X.501 - Models
X.509 - Authentication Framework
X.511 - Abstract Service Definition
X.518 - Procedures for Distributed Operations
X.519 - Protocol Specifications
X.520 - Selected Attribute types
X.521 - Selected Object Classes
X.525 - Replication
X.530 - Use of Systems Management for Administration of the Directory
XLink - Rules for hyperlinks in an XML document
XLL - Previous name for XLink
XML - eXtensible Markup Language
XPath - Rules for addressing internal elements
XPointer - Rules for linking to an XML document
XSL - Extensible Stylesheet Language
XSLT - XSL transformations

ZEN - Zero Effort Networks

Appendix A
Definition of Acronyms

Organizational Terms

ARPA - Advanced Research Projects Agency
DOE NWC - Department of Energy Nuclear Weapons Complex
DMTF - Distributed Management Task Force, Formally the Desktop Management Task Force
IETF - Internet Engineering Task Force
ISO - International Standards Organization
PFWG - Policy Framework Working Group

Sandia Specific Organizational Terms

SNL/CA - Sandia National Laboratories California
SNL/NM - Sandia National Laboratories New Mexico
CSU - Sandia Customer Support Unit

Sandia Specific Technical Terms

ASCI - Accelerated Strategic Computing Initiative
COE - Common Operating Environment
DISCOM - Distance and Distributed Computing
NWIS - NetWork Information System

Sandia Telecommunication Operations ISO 9000 Process

AMP - Asset Management Process
CIP - Continuous Improvement Process
CMP - Change Management Process
DEP - Development & Evaluation Process
DMP - Document Management Process
NMP - Network Management Process
OCP - Organizational Communication Process
OTP - Orientation and Training Process
TRP - Trouble Resolution Process

Appendix B

Sandia Server Consistency Team Standard Server Naming Convention

In 1998 The Sandia National Laboratories Server Consistency Sub Team established the Standard Server Naming Convention.

The SSCT Standard Server Naming Convention is:

FTnnADOS(O) where

FT, a two character designator indicating the server's function type:
AD - Active Directory Server
AS - Application Server
BS - Backup Server
CD - CD Server
CS - Corporate Applications Server
DB - Data Base Server
DC - Domain Controller
DS - Data Server
ES - Exchange Server
FS - Fileserver (ex. ftp)
NS - Name Server (WINS, DNS)
PO - Post Office Server
PS - Print Server
TS - Terminal Server (e.g. Citrix WinFrame)
WS - Web Server
nn, a two position decimal number designating the sequential server number of the specified function type/administrative designator.
AD, a three character administrative designator:
SNL - Corporate server
csu - The administrative CSU's 3 digit number, i.e. (802, 807, 821, 836, 880, 890, 891, 897, 960, A35)
SPL - CSU Special Projects server
PRJ - CSU administered server for a unique project
OS, one of the following two character OS designator:
NT - New Technology
UX - UNIX
AP - Apple
W2 - Windows 2000
CX - CITRIX
VM - VMS
(**O**), a single optional terminating character as follows:
O - Open Network - EON
S - Secure Network - ISN
(If the optional character is not present, by default the server resides on the IRN).

Appendix B

Note: This standard is open-ended. As future requirements dictate additions and extensions to it, it is expected that they will be proposed, reviewed, and decided upon by the SSCT based on their merits at that point in time.

Following are examples of servers using the SSCT standard naming convention:

- WS01SNLNT - The first corporate NT web server on the IRN
- ES04SNLNT - The fourth corporate Exchange server on the IRN
- DC02891NTO - The second CSU891 Domain controller on the EON
- FS01SNLNTS - The first corporate file server on the ISN

Appendix C

Common Naming Convention Reference

Domain Name System (DNS) host and NetBIOS naming
The TCP/IP host name and NetBIOS computer name conventions should be integrated through a common naming strategy. When viewed from the top level a corporate naming strategy for name space and name resolution systems assist in providing integration and management of the enterprise network. Windows Internet Naming Service (WINS) provides NetBIOS name to IP address name resolution in a Microsoft environment. Domain Name System (DNS) provides IP host name to IP address name resolution in a TCP/IP environment. These two functions though similar function independently of each other.

Microsoft NT 4.0 and earlier Microsoft NT systems require NetBIOS computer names. A common name convention for WINS NetBIOS and DNS host names provide applications, end users and system administrators a common system identification.

Several options are presented for Host and NetBIOS Microsoft NT Domain names as examples for a common naming convention.

Directory Service Naming Conventions
Three directory-service naming options are presented.

- Microsoft Windows 2000 Active Directory
- Lightweight Directory Access Protocol
- Novell Directory Services eDirectory

Electronic Mail Common Naming Convention
An Electronic mail naming convention is presented based on the user identification of first initial, middle initial and the first five letters of the users last name. The E-mail common-naming-convention includes Surname, Given name, Organization and location.

Appendix C

Domain Name System Domain Naming

Three DNS naming options are presented for consideration.

- Option 1 presents a naming convention for multiple authoritative domains.
- Option 2 presents a naming convention for a single authoritative domain with virtual sub domains(two part host names).
- Option 3 presents a naming convention for multiple authoritative domains for Microsoft Active Directory.

Domain Name System Common Naming Conventions
Option 1
Multiple Authoritative Domains

DNS Option 1 provides a naming convention for multiple authoritative domains within the enterprise network environment.

Consideration should be given to supporting Directory-service name resolution requirements in DNS, such as Lightweight Directory Access Protocol directory-service URL/Text entries.

Domain Name System Symbol designation: “@” - designates origin, “;” - designates a comment, “NS” - designates the name server, “IN” - designates an Internet record, “A” - designates an IP address, "CNAME" designates a Canonical Name, "HINFO" designates Host information, "MINFO" designates Mailbox or mail list information, "TXT" designates text, "WKS" designates a Well Known Service, "ISDN" designates Integrated Digital Services Network, "NOTIFY" designates notify, "UPDATE" designates Dynamic update, “PTR” designates a reverse lookup pointer record, “MX” - designates a mail exchange record, SRV RR - Service Resource Record format _Service._Proto.Name (i.e. _ldap._tcp.sandia.gov), “WINS” - designates a WINS record for Microsoft DNS WINS lookup, the WINS record is applicable to Microsoft DNS servers only, NSAP RR - Name to ATM NSAP address record, DNSSEC Resource Records - KEY, SIG, NXT.

Domain Name System top-level domains: gov, com, edu, org, net, mil, biz, xx-two letter country code.
Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).

Item	Standard Example	Structure	Example
Authoritative Domain	second level authoritative domain. top-level domain	Authoritative domain, period separator, top-level domain	sandia.gov
Authoritative Sub Domain(s)	third level authoritative sub domain. second level authoritative domain. top-level domain	Authoritative sub-domain, period separator, authoritative domain, period separator, top-level domain	csu880.sandia.gov

Appendix C

Item	Standard Example	Structure	Example
Host name, Authoritative Sub Domain(s)	host name. third level authoritative sub-domain. second level authoritative domain. top-level domain	Host name, period separator, authoritative sub-domain, period separator, authoritative domain, period separator, top-level domain	jtuser01.csu880.sandia.gov jtuserdl.csu880.sandia.gov sadl0911.csu880.sandia.gov

Appendix C

Domain Name System Common Naming Conventions
Option 2
Single Authoritative Domain/Virtual Sub-Domains

DNS Option 2 provides a naming convention for a single authoritative domain and virtual sub-domains within the enterprise network environment.

Consideration should be given to supporting directory-service name resolution requirements in DNS, such as Lightweight Directory Access Protocol directory-service URL/Text entries.

Domain Name System Symbol designation: “@” - designates origin, “;” - designates a comment, “NS” - designates the name server, “IN” - designates an Internet record, “A” - designates an IP address, "CNAME" designates a Canonical Name, "HINFO" designates Host information, "MINFO" designates Mailbox or mail list information, "TXT" designates text, "WKS" designates a Well Known Service, "ISDN" designates Integrated Digital Services Network, "NOTIFY" designates notify, "UPDATE" designates Dynamic update, “PTR” designates a reverse lookup pointer record, “MX” - designates a mail exchange record, SRV RR - Service Resource Record format _Service._Proto.Name (i.e. _ldap._tcp.sandia.gov), “WINS” - designates a WINS record for Microsoft DNS WINS lookup, the WINS record is applicable to Microsoft DNS servers only, NSAP RR - Name to ATM NSAP address record, DNSSEC Resource Records - KEY, SIG, NXT.

Domain Name System top-level domains: gov, com, edu, org, net, mil, biz, xx-two letter country code.
Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).

Item	Standard Example	Structure	Example
Single Authoritative Domain name	second level authoritative domain. top-level domain	Sub-domain, period separator, top-level domain	sandia.gov
Virtual Domains (Two part Host Names) - virtual sub domain name	third level virtual sub domain (two part host name). second level authoritative domain. top-level domain	Sub-domain, period separator, sub-domain, period separator, top-level domain	csu880.sandia.gov
Virtual Domains (Two part Host Names)	(host name. third level virtual domain). second level authoritative domain. top-level domain	Host name, period separator, virtual domain, period separator, authoritative domain, period separator, top-level domain	jtuser01.csu880.sandia.gov jtuserdl.csu880.sandia.gov sadl0911.csu880.sandia.gov

Appendix C

Domain Name System Common Naming Conventions
Option 3
Multiple Authoritative Domains for Active Directory

DNS Option 3 assumes that Microsoft Active Directory will require authoritative sub domains.

Microsoft Windows 2000 relies on DNS to perform Active Directory name resolution based on a Domain tree architecture.

Consideration should be given to supporting directory-service name resolution requirements in DNS, such as Lightweight Directory Access Protocol directory-service URL/Text entries.

Domain Name System Symbol designation: “@” - designates origin, “;” - designates a comment, “NS” - designates the name server, “IN” - designates an Internet record, “A” - designates an IP address, "CNAME" designates a Canonical Name, "HINFO" designates Host information, "MINFO" designates Mailbox or mail list information, "TXT" designates text, "WKS" designates a Well Known Service, "ISDN" designates Integrated Digital Services Network, "NOTIFY" designates notify, "UPDATE" designates Dynamic update, “PTR” designates a reverse lookup pointer record, “MX” - designates a mail exchange record, SRV RR - Service Resource Record format _Service._Proto.Name (i.e. _ldap._tcp.sandia.gov), “WINS” - designates a WINS record for Microsoft DNS WINS lookup, the WINS record is applicable to Microsoft DNS servers only, NSAP RR - Name to ATM NSAP address record, DNSSEC Resource Records - KEY, SIG, NXT.

Domain Name System top-level domains: gov, com, edu, org, net, mil, biz, xx-two letter country code.
Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).

Item	Standard Example	Structure	Example
Authoritative Domain in the Active Directory Domain tree.	second level sub-domain. top-level domain	Sub-domain, period separator, top-level domain	sandia.gov
Authoritative Sub Domain(s) in the Active Directory Domain tree.	third level sub domain. second level sub-domain. top-level domain	Sub domain, period separator, sub-domain, period separator, top-level domain	csu880.sandia.gov
Host Name, Authoritative Sub Domain(s) in the Active Directory Domain tree.	host name. Second level sub-domain. top-level domain	Host name, period separator, sub-domain, period separator, top-level domain	jtuser01.csu880.sandia.gov jtuserdl.csu880.sandia.gov sadl0911.csu880.sandia.gov

Appendix C

Domain Name System (DNS) Host and NetBIOS Naming

Four DNS host and NetBIOS options are presented for consideration.

- Option 1 presents a user ID for a numeric identifier based host/NetBIOS name.
- Option 2 presents a user ID for a machine vendor style system identifier based host/NetBIOS name.
- Option 3 presents a Sandia Albuquerque (SA)XX ID based host/NetBIOS name.
- Option 4 presents a mixed naming strategy for a user ID based convention for NetBIOS, Macintosh and other systems while retaining a SAXX naming convention for UNIX based systems.

The options are presented with three category definitions.

- DNS Name Server, Internet Record & Address entry.
- TCP/IP Host Names
- NetBIOS Names

Domain Name System Host & NetBIOS Names
Option 1

DNS host and NetBIOS option 1 provides that host and NetBIOS names are represented by a user ID based scheme with a numeric system identifier such as “jtuser01” for the users first system, “jtuser02” for the users second system.

DNS Name Server, Internet Record and Address Entry Option 1

Domain Name System Symbol designation: “@” - designates origin, “;” - designates a comment, “NS” - designates the name server, “IN” - designates an Internet record, “A” - designates an IP address, "CNAME" designates a Canonical Name, "HINFO" designates Host information, "MINFO" designates Mailbox or mail list information, "TXT" designates text, "WKS" designates a Well Known Service, "ISDN" designates Integrated Digital Services Network, "NOTIFY" designates notify, "UPDATE" designates Dynamic update, “PTR” designates a reverse lookup pointer record, “MX” - designates a mail exchange record, SRV RR - Service Resource Record format _Service._Proto.Name (i.e. _ldap._tcp.sandia.gov), “WINS” - designates a WINS record for Microsoft DNS WINS lookup, the WINS record is applicable to Microsoft DNS servers only, NSAP RR - Name to ATM NSAP address record, DNSSEC Resource Records - KEY, SIG, NXT.

Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).

Item	Structure	Example
Host Alias Name entry Strategy Option 1 CNAME record	Host name entry Alias entry “host alias name” IN CNAME “host name” If canonical names are represented by a user ID based scheme with a numeric system identifier then alias support would include a functional friendly name (e.g. 880ftp, snlftp, ftp (Location or function should be apparent)). The SAXX name could be supported as an alias (e.g. sadl0911)	jtuser01 IN A 134.253.219.140 880ftp IN CNAME jtuser01, sadl0911 IN CNAME jtuser01

Appendix C

DNS Name Server, Internet Record and Address Entry Option 1 (Continued)			
Item	**Standard Example**	**Structure**	**Example**
Reverse Lookup Pointer Records	IP reverse domain name> IN PTR host name	IP reverse domain name> IN PTR host name	xxx.181.253.134.in-addr.arpa. IN PTR dn880uxp.sandia.gov
DNS Name Servers (Proposed CSU Server Naming Convention)	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	Dn880uxp UNIX primary, dn880uxs secondary, dn880ntp NT primary, dn880nts NT secondary

Appendix C

TCP/IP Host Names Option 1			
Host names will use the primary users seven letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two character numeric identifier. Servers will use the Naming Convention for CSU Servers as defined by the Server Consistency Sub Team. An alias strategy supporting functional and friendly names should be supported. Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).			
Item	**Standard Example**	**Structure**	**Example**
Windows NT server (Proposed CSU Server Naming Convention) Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01snlnt fs01880nt w301880nt po01880nt
Windows NT workstation 3.51	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, jtuser05
Windows NT workstation 4.0	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, jtuser02
Windows 95	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, jtuser03
Apple Macintosh	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, jtuser04
UNIX workstations	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, jtuser06

Appendix C

NetBIOS Names Option 1

NetBIOS computer names will use the primary users seven letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two character numeric identifier.

Servers will use the Naming Convention for CSU Servers as defined by the Server Consistency Sub Team.

File and Print service for NetWare (FPNW) servers will use a two character descriptor for type (e.g. FP - NT FPNW server); a two character alphanumeric designating server number (01-FF (Hex) coinciding with the host NT server designating server number); a three character location (SNL or 880, CSU or building number coinciding with the host NT server designating server location identifier); a two character functional identifier (e.g. PO- PostOffice); and can add a one character special identifier.

The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the designating server number (01), the location identifier 880 (e.g. fp01880) This has the added advantage of ensuring that the FPNW IPX numbers are not placed at the top of routing tables diminishing the possibility of errors caused by responding to get nearest server requests.

Devices such as printers may use a port name such as "Bldg-Room-Mfg-Type" and a location-independent share name. E.g.,
SV-3400-XE-4700C would specify a Xerox 4700 Color printer in room 3400 of the Sandia Vista building.
Meaningful comments are encouraged for both Servers and Devices.

Item	Standard Example	Structure	Example
Windows NT server (Proposed CSU Server Naming Convention) Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01snlnt fs01880nt w301880nt po01880nt
Windows NT Workstation Note: No designation of NT OS version 3.5.1 and 4.0.	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01
Windows 95	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01
Windows For Workgroups	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01

Appendix C

Item	Standard Example	Structure	Example
File and Print service for NetWare (FPNW) implementation.	FF##LLLHH	Two character function identifier (FP), a two character hexadecimal server number identifier (same as the host server), a three character location identifier (same as the host server), a two character host server function identifier. The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the host designating server number, and the location identifier 880 (e.g. fp01880).	fp01880po f01880

Appendix C

Domain Name System Host & NetBIOS Names Option 2
DNS host and NetBIOS option 2 provides that host and NetBIOS names are represented by an user ID based scheme with SAXX style system identifier such as “jtuserdl” for a Dell system, “jtusermt” for Macintosh system, “jtuserhp” for an Hewlett Packard system and “jtuserss” for a Sun SPARC system.

DNS Name Server, Internet Record and Address Entry Option 2
Domain Name System Symbol designation: “@” - designates origin, “;” - designates a comment, “NS” - designates the name server, “IN” - designates an Internet record, “A” - designates an IP address, "CNAME" designates a Canonical Name, "HINFO" designates Host information, "MINFO" designates Mailbox or mail list information, "TXT" designates text, "WKS" designates a Well Known Service, "ISDN" designates Integrated Digital Services Network, "NOTIFY" designates notify, "UPDATE" designates Dynamic update, “PTR” designates a reverse lookup pointer record, “MX” - designates a mail exchange record, SRV RR - Service Resource Record format _Service._Proto.Name (i.e. _ldap._tcp.sandia.gov), “WINS” - designates a WINS record for Microsoft DNS WINS lookup, the WINS record is applicable to Microsoft DNS servers only, NSAP RR - Name to ATM NSAP address record, DNSSEC Resource Records - KEY, SIG, NXT. Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).

Item	Structure	Example
Host Alias Name entry Strategy Option 2 CNAME record	Host name entry Alias entry “host alias name” IN CNAME “host name” If canonical names are represented by a user ID based scheme with a SAXX style system identifier then alias support would include a functional friendly name (e.g. 880ftp, snlftp, ftp (Location or function should be apparent)). The SAXX name could be supported as an alias (e.g. sadl0911)	jtuserdl IN A 134.253.219.140 880ftp IN CNAME jtuserdl, sadl0911 IN CNAME jtuserdl

Item	Standard Example	Structure	Example
Reverse Lookup Pointer Records	IP reverse domain name> IN PTR host name	IP reverse domain name> IN PTR host name	xxx.181.253.134.in-addr.arpa. IN PTR dn880uxp.sandia.gov
DNS Name Servers (Proposed CSU Server Naming Convention)	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	Dn880uxp UNIX primary, dn880uxs secondary, dn880ntp NT primary, dn880nts NT secondary

Appendix C

TCP/IP Host Names Option 2			
Host names will use the primary users seven letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two character system identifier. CSU servers will use the Naming Convention for CSU Servers as defined by the Server Consistency Sub Team. An alias strategy supporting functional and friendly names should be supported. Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).			
Item	**Standard Example**	**Structure**	**Example**
Windows NT server (Proposed CSU Server Naming Convention) Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01snlnt fs01880nt w301880nt po01880nt
Windows NT workstation 4.0	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows 95	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows NT workstation 3.51	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Apple Macintosh	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtusermt
UNIX workstations	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserss, jtusersg

Appendix C

NetBIOS Names Option 2

NetBIOS computer names will use the primary users seven letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two character system identifier.

CSU servers will use the Naming Convention for CSU Servers as defined by the Server Consistency Sub Team.

File and Print service for NetWare (FPNW) servers will use a two character descriptor for type (e.g. FP - NT FPNW server); a two character alphanumeric designating server number (01-FF (Hex) coinciding with the host NT server designating server number); a three character location (SNL or 880, CSU or building number coinciding with the host NT server designating server location identifier); a two character functional identifier (e.g. PO- PostOffice); and can add a one character special identifier.

The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the designating server number (01), the location identifier 880 (e.g. fp01880) This has the added advantage of ensuring that the FPNW IPX numbers are not placed at the top of routing tables diminishing the possibility of errors caused by responding to get nearest server requests.

Devices such as printers may use a port name such as "Bldg-Room-Mfg-Type" and a location-independent share name. E.g.,
SV-3400-XE-4700C would specify a Xerox 4700 Color printer in room 3400 of the Sandia Vista building.
Meaningful comments are encouraged for both Servers and Devices.

Item	Standard Example	Structure	Example
Windows NT server (Proposed CSU Server Naming Convention) Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01snlnt fs01880nt w301880nt po01880nt
Windows NT Workstation Note: No designation of NT OS version 3.5.1 and 4.0.	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows 95	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp
Windows For Workgroups	fmnnnnn##	First initial, middle initial, first five letters of the last name, two character system identifier.	jtuserdl, jtuserhp

Appendix C

Item	Standard Example	Structure	Example
File and Print service for NetWare (FPNW) implementation.	F##LLLHH	Two character function identifier (FP), a two character hexadecimal server number identifier (same as the host server), a three character location identifier (same as the host server), a two character host server function identifier. The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the host designating server number, and the location identifier 880 (e.g. fp01880).	fp01880po f01880

Appendix C

Domain Name System Host & NetBIOS Names Option 3
DNS host and NetBIOS option 3 provides that host and NetBIOS names are represented the SAXX style naming convention system identifier such as sahp621 - for a Hewlett Packard PC, sadl768 - for a Dell PC, samt256 - for a Macintosh, or sass1028 - for a Sun SPARC workstation. Note: The SAXX naming convention should be revised to meet current requirements for system identification. Specifically the “ix” system identifier does not uniquely identify systems. The current NWIS system assigns SAXX ID’s with the system identifier of “ix” for dec, hp, ibm, and ibm thinkpad personal computers, as well as a host of other PC manufacturers and non PC systems. This specification should be revised to represent unique system identifiers, should this naming strategy be adopted.

DNS Name Server, Internet Record and Address Entry Option 3
Domain Name System Symbol designation: “@” - designates origin, “;” - designates a comment, “NS” - designates the name server, “IN” - designates an Internet record, “A” - designates an IP address, "CNAME" designates a Canonical Name, "HINFO" designates Host information, "MINFO" designates Mailbox or mail list information, "TXT" designates text, "WKS" designates a Well Known Service, "ISDN" designates Integrated Digital Services Network, "NOTIFY" designates notify, "UPDATE" designates Dynamic update, “PTR” designates a reverse lookup pointer record, “MX” - designates a mail exchange record, SRV RR - Service Resource Record format _Service._Proto.Name (i.e. _ldap._tcp.sandia.gov), “WINS” - designates a WINS record for Microsoft DNS WINS lookup, the WINS record is applicable to Microsoft DNS servers only, NSAP RR - Name to ATM NSAP address record, DNSSEC Resource Records - KEY, SIG, NXT. Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).

Item	Structure	Example
Host Alias Name entry Strategy Option 3 CNAME record	Host name entry Alias entry “host alias name” IN CNAME “host name” If canonical names are represented by the SAXX style scheme then alias support would include a functional or friendly name (e.g. 880ftp, snlftp, ftp (Location or function should be apparent)). The user ID based name could be supported as an alias (e.g. jtuser01)	sadl0911 IN A 134.253.219.140 880ftp IN CNAME sadl0911, jtuser01 IN CNAME sadl0911

Item	Standard Example	Structure	Example
Reverse Lookup Pointer Records	IP reverse domain name> IN PTR host name	IP reverse domain name> IN PTR host name	xxx.181.253.134.in-addr.arpa. IN PTR dn880uxp.sandia.gov

Appendix C

Item	Standard Example	Structure	Example
DNS Name Servers (Proposed CSU Server Naming Convention)	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	Dn880uxp UNIX primary, dn880uxs secondary, dn880ntp NT primary, dn880nts NT secondary

Appendix C

TCP/IP Host Names Option 3			
Host names will use the Sandia assigned system identifier resulting from a two character Sandia Albuquerque/Livermore identifier, two character system type identifier, four character numeric identifier. The standard would be consistent for NetBIOS naming and host naming. CSU servers will use the Naming Convention for CSU Servers as defined by the Server Consistency Sub Team. An alias strategy supporting functional and friendly names should be supported. Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).			
Item	**Standard Example**	**Structure**	**Example**
Windows NT server (Proposed CSU Server Naming Convention) Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01snlnt fs01880nt w301880nt po01880nt
Windows NT workstation 4.0	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (dl, hp) four character numeric identifier.	Sahp0621 - for a Hewlett Packard PC, sadl0621 - for a Dell PC
Windows NT workstation 3.51	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (dl, hp) four character numeric identifier.	Sahp0621 - for a Hewlett Packard PC, sadl0621 - for a Dell PC
Windows 95	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (dl, hp) four character numeric identifier.	Sahp0768 - for a Hewlett Packard PC, sadl0621 - for a Dell PC
Apple Macintosh	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (mt) four character numeric identifier.	Samt0256
UNIX workstations	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (sg, ss) four character numeric identifier.	Sass0768 - for Sun SPARC station, sasg0621 - for a Silicon Graphics system.

Appendix C

NetBIOS Names Option 3

NetBIOS computer names will use the Sandia assigned system identifier resulting from a two character Sandia Albuquerque/Livermore identifier, two character system type identifier, four character numeric identifier.

CSU servers will use the Naming Convention for CSU Servers as defined by the Server Consistency Sub Team.

File and Print service for NetWare (FPNW) servers will use a two character descriptor for type (e.g. FP - NT FPNW server); a two character alphanumeric designating server number (01-FF (Hex) coinciding with the host NT server designating server number); a three character location (SNL or 880, CSU or building number coinciding with the host NT server designating server location identifier); a two character functional identifier (e.g. PO- PostOffice); and can add a one character special identifier.

The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the designating server number (01), the location identifier 880 (e.g. fp01880) This has the added advantage of ensuring that the FPNW IPX numbers are not placed at the top of routing tables diminishing the possibility of errors caused by responding to get nearest server requests.

Devices such as printers may use a port name such as "Bldg-Room-Mfg-Type" and a location-independent share name. E.g.,
SV-3400-XE-4700C would specify a Xerox 4700 Color printer in room 3400 of the Sandia Vista building.
Meaningful comments are encouraged for both Servers and Devices.

Item	Standard Example	Structure	Example
Windows NT server (Proposed CSU Server Naming Convention) Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01snlnt fs01880nt w301880nt po01880nt
Windows NT workstation 4.0	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (dl, hp) four character numeric identifier.	Sahp0621 - for a Hewlett Packard PC, sadl0621 - for a Dell PC
Windows NT workstation 3.51	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (dl, hp) four character numeric identifier.	sahp0621 - for a Hewlett Packard PC, sadl0621 - for a Dell PC
Windows 95	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (dl, hp) four character numeric identifier.	Sahp0621 - for a Hewlett Packard PC, sadl0621 - for a Dell PC
Windows For Workgroups	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (dl, hp) four character numeric identifier.	sahp0621 - for a Hewlett Packard PC, sadl0621 - for a Dell PC

Appendix C

NetBIOS Names Option 3 Continued			
File and Print service for NetWare (FPNW) implementation.	FF##LLLHH	Two character function identifier (FP), a two character hexadecimal server number identifier (same as the host server), a three character location identifier (same as the host server), a two character host server function identifier. The IPX number assignment for FPNW servers should reflect the server function (f-FPNW), the host designating server number, and the location identifier 880 (e.g. fp01880).	fp01880po f01880

Appendix C

Host Names Option 4			
Host names representing Microsoft NetBIOS systems will use the primary users seven letter login name consisting of first initial, middle initial, then the first five letters of the last name and a two character numeric or system identifier. Host names representing UNIX systems will use the Sandia assigned system identifier resulting from a two character Sandia Albuquerque/Livermore identifier, two character system type identifier, four character numeric identifier. CSU servers will use the Naming Convention for CSU Servers as defined by the Server Consistency Sub Team. An alias strategy supporting functional and friendly names should be supported. Typical DNS and host names allow for the use of the following characters: “a-z”, “A-Z”, “0-9” “-“ (dash or minus sign).			
Item	**Standard Example**	**Structure**	**Example**
Windows NT server (Proposed CSU Server Naming Convention) Note: No designation of NT OS version 3.5.1 and 4.0.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01snlnt fs01880nt w301880nt po01880nt
Windows NT workstation 4.0	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserdl (Dell)
Windows NT workstation 3.51	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserdl (Dell)
Windows 95	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserdl (Dell)
Apple Macintosh	fmnnnnn## The primary users ID	First initial, middle initial, first five letters of the last name, two character numeric identifier.	jtuser01, or jtuserap (Apple)
UNIX workstations	SAXX####	Two character Sandia Albuquerque/Livermore identifier (sa, sl), two character system type identifier (mt, ix, dl, hp, no, ss) four character numeric identifier.	sass1028 - for a Sun SPARC station

Appendix C

Naming Convention For CSU Servers			
Servers will use a two character descriptor for type (e.g. PO - PostOffice, FS - File Server, FT - FTP Server, PS - Print Server, DS - Data Server, CS - Corporate Application Server, BS - Backup Server, , DC - Data Cluster); a two character hexadecimal designating server number (01-FF); a three character location identifier (SNL or 880 (CSU or building number)); a two character OS identifier (NT, UX, NW, AP); and can add an optional one character special identifier.			
Item	**Standard Example**	**Structure**	**Example**
Windows NT server 3.5.1	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	po01880nt3, ds01snlnt
Windows NT server 4.0	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	cs01880nt, ds01snlnt
Novell 3.12 servers	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds01880nw
Novell 4 servers	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds02880nw4
FTP servers TFTP servers WWW servers Gopher servers LDAP Master servers LDAP Slave servers	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ft01880nt tf01880nt w301880nt gs01880nt lm01880nt ls01880nt

Appendix C

Microsoft NT Domain Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
Master Microsoft NT domain(s) name whose name is based on the Sandia National Laboratories organization.	OOOOOO	Up to seven character descriptive organization name.	sandia sandia2 (multimaster)
Resource Microsoft NT domain name whose name is based on a CSU location.	CSU### or CSUX##	"CSU" Prefix, CSU identifier.	CSU807 or CSUA35
Resource Microsoft NT domain name whose name is based on an SNL organization.	#### or #####	Four or five character organization number.	7000, 15000, 04911

Microsoft NT Share Names Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
Corporate Microsoft NT share names	Meaningful content	Up to eight character descriptive name.	\\ds01snlnt\SOURCE
Independent Microsoft NT share names.	Meaningful content	Up to eight character descriptive name.	\\servername\PUBSHARE

Appendix C

Directory Service Naming Conventions

Three directory-service naming conventions are presented - Microsoft Active Directory, Lightweight Directory Access Protocol and Novell Directory Services eDirectory

Microsoft Active Directory Service Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
User object common name (login name)	fmnnnnn Note: Microsoft NT users names restricted to 20 characters, restricted characters / \ [ ] : ; | = , + * ? < >	Seven letter login name consisting of first and middle initial, then the first five letters of the last name.	jtuser
User object full name	Ffffff M Nnnnnnn	All characters of the first and last name with middle initial. Use initial capitals. No initial punctuation will used.	Joe T User
Given name	Fffffff	First name	Joe
Surname	Lllllll	Last Name	User
Email name	Fmnnnnn@subdomain .top-level domain	Seven letter login name consisting of first and middle initial, then the first five letters of the last name, @, SNL domain, period separator, government domain.	Jtuser@sandia.gov
User object Telephone and Fax	###-###-####	Area code, dash, prefix, dash, extension.	505-845-9483
User object Location	BBB-RRR-MMMM	Building-Room- Mail stop.	859-C2C-0801
Active Directory Domain tree name	OOO_DDTREE	Three letter organization abbreviation, underscore, two character tree identifier (MD=Microsoft Directory)TREE.	SNL_MDTREE
Active Directory Domain Component	Sub-domain.top-level domain	DNS naming	sandia.gov
Active Directory Domain name CSU based	CSU### or CSUX##	“CSU” Prefix, CSU identifier.	CSU807 or CSUA35.sandia.gov
Active Directory Domain name Organization based	#### or #####	Four or five character organization number.	7000, 15000,0 or 04911.sandia.gov
Country object name	CC	Two character Country identifier.	US
Organization object name	OOO	Three letter organization abbreviation.	SNL
Organization Unit object name whose name is based on a state location.	OOOLL	Three letter organization abbreviation. Two character location identifier.	SNLNM, SNLCA
Organizational Unit object name whose name is based on a tech area location.	TA### or TA###-#	“TA” prefix, roman numeral designation.	TAI, TAIV or TAIII-V

Appendix C

Microsoft Active Directory Service Common Naming Conventions (Continued)			
Item	**Standard Example**	**Structure**	**Example**
Organizational Unit object name whose name is based on a CSU location.	CSU### or CSUX##	"CSU" Prefix, CSU identifier.	CSU807 or CSUA35
Organizational Unit object name whose name is based on an SNL Organization.	#### or #####	Four or five character organization number.	7000, 15000, 04911
Application object name	VVAAAA###	Two character vendor identifier, four character Application description, three character version identifier.	NSW3BR003 (Netscape WWW Browser version 3)
Printer object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PR-T550-880-C48 c 880-C48-X47C-PR
Print Queue object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PQ-T550-880-C48 c 880-C48-X47C-PQ
Print Server object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PS-T550-880-C48 c 880-C48-X47C-PS
Server object name Unique company wide.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds02880nw4
All common names	Avoid special characters (+=/ \) and spaces.		

Appendix C

Lightweight Directory Access Protocol Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
User object common name (login name)	fmnnnnn	Seven letter login name consisting of first and middle initial, then the first five letters of the last name.	jtuser
User object full name	Ffffff M Nnnnnnn	All characters of the first and last name with middle initial. Use initial capitals. No initial punctuation will used.	Joe T User
Given name	Fffffff	First name	Joe
Surname	Lllllll	Last Name	User
Email name	fmnnnnn.subdomain .top-level domain	Seven letter login name consisting of first and middle initial, then the first five letters of the last name, @, SNL domain, period separator, government domain.	Jtuser@sandia.gov
User object Telephone and Fax	###-###-####	Area code, dash, prefix, dash, extension.	505-845-9483
User object Location	BBB-RRR-MMMM	Building-Room- Mail stop.	859-C2C-0801
Directory tree name	OOO_DDTREE	Three letter organization abbreviation, underscore, two character tree identifier (LD=LDAP Directory)TREE.	SNL_LDTREE
Country object name	CC	Two character Country identifier.	US
Organization object name	OOO	Three letter organization abbreviation.	SNL
Organization Unit object name whose name is based on a state location.	OOOLL	Three letter organization abbreviation. Two character location identifier.	SNLNM, SNLCA
Organizational Unit object name whose name is based on a tech area location.	TA### or TA###-#	“TA” prefix, roman numeral designation.	TAI, TAIV or TAIII-V
Organizational Unit object name whose name is based on a CSU location.	CSU### or CSUX##	“CSU” Prefix, CSU identifier.	CSU807 or CSUA35
Organizational Unit object name whose name is based on an SNL Organization.	#### or #####	Four or five character organization number.	7000, 15000, 04911
Application object name	VVAAAA###	Two character vendor identifier, four character Application description, three character version identifier.	NSW3BR003 (Netscape WWW Browser version 3)

Appendix C

Lightweight Directory Access Protocol Common Naming Conventions (Continued)			
Item	**Standard Example**	**Structure**	**Example**
Printer object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PR-T550-880-C48 or 880-C48-X47C-PR
Print Queue object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PQ-T550-880-C48 or 880-C48-X47C-PQ
Print Server object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PS-T550-880-C48 880-C48-X47C-PS
Server object name Unique company wide.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds02880nw4
All common names	Avoid special characters (+=/ \) and spaces.		

Appendix C

Novell Directory Services Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
User object common name (login name)	fmnnnnn	Seven letter login name consisting of first and middle initial, then the first five letters of the last name.	jtuser
User object full name	Ffffff M Nnnnnnn	All characters of the first and last name with middle initial. Use initial capitals. No initial punctuation will used.	Joe T User
Given name	Fffffff	First name	Joe
Surname	Lllllll	Last Name	User
Email name	fmnnnnn.subdomain .top-level domain	Seven letter login name consisting of first and middle initial, then the first five letters of the last name, @, SNL domain, period separator, government domain.	Jtuser@sandia.gov
User object Telephone and Fax	###-###-####	Area code, dash, prefix, dash, extension.	505-845-9483
User object Location	BBB-RRR-MMMM	Building-Room- Mail stop.	859-C2C-0801
Directory tree name	OOO_DDTREE	Three letter organization abbreviation, underscore, two character tree identifier (ND=Novell Directory)TREE.	SNL_NDTREE
Country object name	CC	Two character Country identifier.	US
Organization object name	OOO	Three letter organization abbreviation.	SNL
Organization Unit object name whose name is based on a state location.	OOOLL	Three letter organization abbreviation. Two character location identifier.	SNLNM, SNLCA
Organizational Unit object name whose name is based on a tech area location.	TA### or TA###-#	“TA” prefix, roman numeral designation.	TAI, TAIV or TAIII-V
Organizational Unit object name whose name is based on a CSU location.	CSU### or CSUX##	“CSU” Prefix, CSU identifier.	CSU807 or CSUA35
Organizational Unit object name whose name is based on an SNL Organization.	#### or #####	Four or five character organization number.	7000, 15000, 04911
Application object name	VVAAAA###	Two character vendor identifier, four character Application description, three character version identifier.	NSW3BR003 (Netscape WWW Browser version 3)

Appendix C

Novell Directory Services Common Naming Conventions (Continued)			
Item	**Standard Example**	**Structure**	**Example**
Printer object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PR-T550-880-C48 or 880-C48-X47C-PR
Print Queue object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PQ-T550-880-C48 or 880-C48-X47C-PQ
Print Server object name Unique company wide.	OO-DDDD-BBB-RRR or BBB-RRR-DDDD-OO (depending on browsing preference)	Two character object class, dash, four character brand or Department, dash, three character Bldg., dash, three character room. or Three character Bldg., dash, three character room, dash, four character brand or Department, dash, two character object class.	PS-T550-880-C48 or 880-C48-X47C-PS
Server object name Unique company wide.	FF##LLLOO?	Two character function identifier, a two character hexadecimal server number identifier, a three character location identifier, a two character OS identifier, and one optional special character.	ds02880nw4
Unique IPX internal /external network number	CCCS###P	3 character CSU number - 1 character server number designation - 3 character unique IPX assignment -1 character protocol, internal IPX number, or virtual NWIP IPX number indicator.	807F1232 (802.2) 807F1233 (802.3) 807F123A (SNAP) 807F1235 (Token Ring) 807F1230 (Internal) 807F1231 (NWIP/IPX)
All common names	Avoid special characters (+=/ \) and spaces.		

Appendix C

Electronic Mail Common Naming Conventions			
Item	**Standard Example**	**Structure**	**Example**
User common name (login name)	fmnnnnn	Seven letter login name consisting of first initial, middle initial, then the first five letters of the last name.	jtuser
Email name	fmnnnnn.subdomain .top-level domain	Seven letter login name consisting of first and middle initial, then the first five letters of the last name, @, SNL domain, period separator, government domain.	Jtuser@sandia.gov
User full name	Ffffff M Nnnnnnn	All characters of the first and last name with middle initial. Use initial capitals. No initial punctuation will used.	Joe T User
Given name	Fffffff	First name	Joe
Surname	Lllllll	Last Name	User
User object Telephone and Fax	###-###-####	Area code-prefix-extension.	505-845-9483
User object Location	BBB-RRR-MMMM	Building-Room- Mail stop.	859-C2C-0801
Organization name	OOOLL	Three letter organization abbreviation. Two character location identifier.	SNLNM, SNLCA
SNL Organization	#### or #####	Four or five character organization number.	7000, 15000, 04911
All common names	Avoid special characters (+=/ \) and spaces.		

Appendix D

NetWork Information System Naming Convention		
The current NWIS naming convention specifies a two character location identifier (e.g. SA - Sandia Albuquerque, SL - Sandia Livermore), a two character Machine_type identifier (e.g. Apple - mt, HP,DEC PC - ix, Dell PC - dl), and a four character numeric identifier. example; sadl1807.		
Machine_make	**Vendor**	**Machine_type Identifier**
net builder	3 comm	tc
link builder	3 comm	tc
terminal svr	3 comm	tc
unknown	abekas	ab
acs	acc	ac
terminal svr	acomm	tc
SNAPS	adaptive solns	as
pc	alr	ix
UPS	american power	am
pc	amerstamp	ix
pc	amiga	ix
powerbook	apple	mt
powermac	apple	mt
printer	apple	mt
macintosh	apple	mt
quadra	apple	mt
pc	aquila	ix
pc	ariel	ix
hub	asante	ae
pc	at&t	at
bridge	bay networks	sp
hub	bay networks	sp
nms	bay networks	sp
pc	bear	ix
hub	cabletron	ct
printer	calcomp	pr
pc	caliber	ix
catalyst	cisco	cc
lightstream	cisco	ls
router	cisco	cr
switch	cisco	cs
pc	clone	ix
printer	clone	pr
workstation	clone	sn

Appendix D

Machine_make	Vendor	Machine_type Identifier
hawk2	club	cl
printer	codonics	cd
pc	color age	ca
bridge	combinet	cb
pc	commodore	cm
pc	compaq	cp
server	compaq	cp
pc	compatible sys	co
router	compatible sys	co
pc	compuadd	ix
pc	cornell	in
ymp	cray	cy
j9	cray	cj
pc	cyntax	ix
badge prntr	datacard	bp
pc	dataexpress	ix
pc	datapro	ix
printer	dataproducts	dp
alpha	dec	da
decstation	dec	ds
pc	dec	ix
printer	dec	dp
vax-ultrix	dec	vu
vax-vms	dec	vv
vaxstation	dec	ds
x-terminal	dec	dt
hub	dec	dh
server	dec	ds
pc	dell	dl
de650	dlink	de
laptop	eps	ix
pc	epson	ix
printer	epson	pr
pc	equus	ix
print server	extended sys.	ex
cpu board	force	fo
pc	force	fo
atm switch	fore	fs

Appendix D

Machine_make	Vendor	Machine_type Identifier
pc	forefront	ix
printer	fujitsu	fu
pc	gateway	gw
bridge	gator box	gb
pc	hauppauge	ha
viewstation	hds	hd
nitro 60	heurikon	hk
file server	hp	hp
pc	hp	ix
plotter	hp	hp
printer	hp	hp
workstation	hp	hp
ws	hp	hx
x-terminal	hp	hx
netserver	hp	hp
omnibook	hp	hp
hub	hp	hp
workstation	hp/apollo	ap
unix clone	huntsville	uc
docking stn	ibm	do
pc	ibm	ix
printer	ibm	pr
x-terminal	ibm	ix
workstation	ibm	ux
mainframe	ibm	ib
server	ibm	is
risc	ibm	ir
thinkpad	ibm	ix
xr655	imp	ip
pc	intel	in
paragon	intel	pa
workstation	intergraph	ig
pc	jdr	ix
switch	kalpana	ka
bridge	kinetics	kb
printer	kodak	kp
print server	lantronix	la
terminal svr	lantronix	la

Appendix D

Machine_make	Vendor	Machine_type Identifier
printer	laser	lp
printer	lodonics	lo
server	logicraft	lc
pc	masscomp	mc
pc	matrix	ms
pc	mcdata	md
pc	metro	ix
pc	micron	ix
plotter	milan	mi
workstation	mips	mp
pc	monolithic	mn
pc	motorola	mr
nes	motorola	en
gpib	national inst	ne
x-terminal	ncd	nt
pc	ncr	ix
pc	nec	ix
FAST mp	netpower	mp
FAST server	netpower	ix
file server	network appl	na
sniffer	network general	ng
workstation	next	nx
pc	northgate	ix
lantern	novell	no
en641	nsc	ne
fe640	nsc	fe
n	nsc	fr
voicemail	octel	oc
pc	packard bell	ix
bridge	pairgain	pg
pc	pcs limited	ix
rpd	polywell	py
pc	premio	ix
printer	printek	pt
printer	qms	qm
pc	radio shack	ix
britlite	rdi	sk
net hopper	rockwell	nh

Appendix D

Machine_make	Vendor	Machine_type Identifier
printer	seiko	se
workstation	sgi	sg
router	shiva	sh
pc	silicon shack	ix
pc	solbourne	sb
printer	sun	si
workstation	sun	sn
pc	sun	sr
terminal svr	sun	st
ultra	sun	ss
sparc	sun	ss
sparcbook	sun	sk
pc	sunnyvale	ix
x/41	super wrkstn	sw
printer	talaris	ta
printer	tektronix	tp
terminal	tektronix	tk
pc	thor	ix
pc	ti	ix
pc	toshiba	ix
pc	touche	ix
server	tricord	tr
printer	unity	un
hub	us robotics	us
pc	vista	ix
pc	wang	wa
pc	western	ix
pc	wyse	ix
printer	xante	xa
printer	xerox	xp
server	xyplex	xy
terminal svr	xyplex	xy
pc	zenith	ze
pc	zenon	ix
pc	zeos	ix

DISTRIBUTION

0801 M. O. Vahle, 09300
0803 H.L. Pitts, 09600
0812 M.R. Sjulin, 09334
0661 G. E. Rivord, 09510
0812 M. D. Gomez, 09334
0812 B. C. Whittet, 09334
0812 C. M. Keliiaa, 09334 (10)
0812 E. J. Klaus, 09334
0812 R. L. Adams, 09334
0812 J. M. Vaughan, 09334
0812 V. K. Williams, 09334
0812 P. M. Torrez, 09334
0812 P. L. Manke, 09334
0812 D. P. Evans, 09334
0812 D. B. Bateman, 09334
0812 D. H. Jensen, 09334
0812 J. H. Maestas, 09334
0812 R. L. Adams, 09334
0812 A. Van Arsdall, 09334
0806 C. D. Brown, 09332
0806 G. D. Machin, 09332
0806 S. A. Gossage, 09336
0806 L. F. Tolendino, 09336
0806 J. A. Hudson, 09336
0806 R. L. Hartley, 09336
0806 M. M. Miller, 09336
0806 T. D. Tarman, 09336
0805 D. J. Bragg, 09329
0805 M. A. Cinense, 09329
0805 J. W. Crenshaw, 09329
0805 T. L. MacAlpine, 09329
0805 R. A. Pastorek, 09329
0805 M. A. Stilwell, 09329
0805 G. K. Rogers, 09329
0805 M. W. Gutscher, 09329
0805 J. M. Muntz, 09329
0805 D. G. Chacon, 09329
0805 C. L. Stein, 09329
0805 J. M. Kreisle, 09329
0805 K. F. Hammond, 09329
0805 P. S. Kuhlman, 09329
0805 J. C. West, 09329
0660 D. S. Cuyler, 09519
0660 P. B. Milligan, 09522
0661 R. M. Harris, 09512
0661 J. R. K. Smith, 09512
0662 D. S. Rogers, 09623
0807 K. E. Wiegandt, 09624
0662 M. D. Snitchler, 09624
0662 J. C. Kelly, 09624
0662 C. A. Quintana, 09624
0801 F. W. Mason, 09320
0813 R. M. Cahoon, 09327
0813 D. P. Patrick, 09327
0813 G. W. Bollig, 09327
0813 R. G. Hawkins, 9327
0813 R. A. Suppona, 09327
0813 A. A. Quintana, 09327
0813 J. W. Morris, 09327
0805 G. L. Esch, 09523
9012 R. D. Gay, 08930
0455 S. V. Spires, 06517
0455 B. M. Nation, 06517
0449 D. E. Ellis, 06516
0785 J. D. Dillinger, 06516
1137 P. C. Moore, 06535
0817 J. C. Hutchins, 09515
9018 Central Technical Files, 8945-1
0899 Technical Library, 9616 (2)
0612 Review and Approval Desk, 09612
for DOE/OSTI